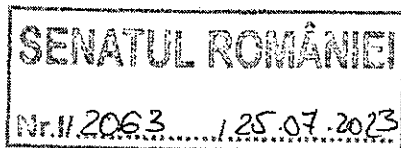




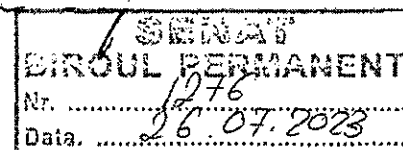
ROMÂNIA
AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE
A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

ANS
PDCP

BM.Gen. Gheorghe Măgheru Nr. 26-30, Sector 1, Cod poștal 010336, București; Tel: +40.31.236.9211; Fax: +40.31.805.9502 www.datiaprotectiei.ro e-mail: anspln@dataprotectie.ro

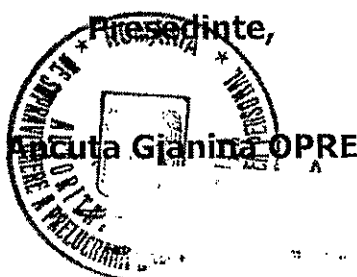


Stimate Doamnă Președinte,



Am deosebita onoare de a supune atenției dumneavoastră Raportul de activitate aferent anului 2022, în conformitate cu dispozițiile art. 5 din Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată.

Cu aleasă prețuire,



Domnului Nicolae CIUCĂ
Președintele Senatului
SENATUL ROMÂNIEI

CUVĂNT ÎNAINTE

Stimate Domnule Președinte al Senatului,

Stimați Senatori,

Am deosebita onoare de a vă prezenta principalele coordonate ale activității Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal în anul 2022, care are ca obiectiv primordial protecția datelor cu caracter personal.

Ne aflăm într-o perioadă de consolidare a aplicării reglementărilor europene în domeniul protecției datelor cu caracter personal, efect al aplicabilității directe, începând cu data de 25 mai 2018, a Regulamentului (UE) 2016/679 privind protecția persoanelor fizice față de prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/EC (Regulamentul General privind Protecția Datelor), adoptat de către Consiliul și Parlamentul European, dar și al aplicării celorlalte legi naționale în domeniu.

În contextul revenirii la activitatea obișnuită după pandemia care ne-a afectat, am sesizat preocuparea operatorilor din mediul public și privat pentru aplicarea regulilor de utilizare a datelor personale, destinate respectării drepturilor persoanelor fizice și asigurării confidențialității și securității prelucrărilor de date personale, inclusiv prin menținerea modalităților specifice de lucru on-line.

Preocupările instituției noastre de asigurarea a unei efective aplicări a normelor europene în mediul digital actual s-au reflectat și în cadrul conferinței anuale dedicată Zilei Europene a Protecției Datelor celebrată pe data de 28 Ianuarie 2022.

În considerarea atribuțiilor naționale de supraveghere de monitorizare și control al respectării regulilor de prelucrare a datelor personale, subliniem că, în anul 2022, au continuat acțiunile de control la nivelul operatorilor din sectorul public și privat, din oficiu sau pe baza plângerilor și sesizărilor primite. În acest sens, am remarcat că plângerile primite din partea persoanelor fizice au fost similare cu cele anterioare, referindu-se, în principal, la dezvăluirea neautorizată a datelor cu caracter personal, la încălcarea drepturilor persoanelor vizate, la aplicarea principiilor de folosire a datelor, la

primirea de mesaje comerciale nesolicitate sau la aplicarea măsurilor de securitate și confidențialitate a prelucrărilor de date personale.

Măsurile corective dispuse au urmărit, cu prioritate, remedierea disfuncționalităților apărute în activitatea operatorilor astfel încât să fie diminuată afectarea drepturilor persoanelor fizice.

Pe un alt palier, instituția noastră a continuat activitatea de informare a publicului larg, cu privire la aplicarea adecvată a regulilor de utilizare a datelor cu caracter personal, în cadrul cărora s-au înscris participarea la evenimente și comunicatele de presă care au reflectat măsurile adoptate și punctele de vedere ale instituției noastre.

Pe planul colaborării cu celelalte autorități naționale de protecția datelor, putem reliefa menținerea acesteia la un nivel constant în ceea ce privește componenta de soluționare a cazurilor cu impact transfrontalier și a transferurilor.

Un moment semnificativ al acestui an l-a constituit misiunea de evaluare Schengen din luna octombrie, care a confirmat încă o dată că Autoritatea națională de supraveghere deține deplina capacitate administrativă și instituțională pentru îndeplinirea exigențelor acquis-ului Schengen.

Raportat la obiectivele instituției noastre, putem aprecia că acestea au fost îndeplinite în condițiile constrângerilor bugetare cu care ne confruntăm și care au generat prestime pe resursele umane limitate disponibile.

În perspectivă, Autoritatea națională de supraveghere își propune continuarea activității de monitorizare și control a operatorilor din sectorul public și privat, intensificarea activitățile de informarea publică a persoanelor fizice, operatorilor și mass-mediei, corelat cu resursele disponibile, în vederea determinării unei aplicări adecvate a Regulamentului (UE) 2016/679 și a celorlalte acte normative aplicabile.

În încheiere, aș dori să vă mulțumesc pentru sprijinul acordat instituției noastre și să-mi exprim încrederea că vom beneficia și pe viitor de susținerea dumneavoastră, în misiunea noastră de consolidare a aplicării principiilor specifice protecției datelor cu caracter personal în România.



CUPRINS

| | | |
|-----------------------------------------------------------------------------------|---------|----------|
| PREZENTARE GENERALĂ..... | pag. 5 | |
| CAPITOLUL I | | |
| ACTIVITATEA DE REGLEMENTARE, AVIZARE, CONSULTARE ȘI INFORMARE PUBLICĂ | | |
| Secțiunea 1 Avizarea actelor normative..... | pag. 8 | |
| Secțiunea a 2-a Puncte de vedere privind diverse chestiuni de protecția datelor.. | pag. 23 | |
| Secțiunea a 3-a Activitatea de reprezentare în fața instanțelor de judecată..... | pag. 43 | |
| Secțiunea a 4-a Informare publică | pag. 57 | |
| CAPITOLUL III | | |
| ACTIVITATEA DE MONITORIZARE ȘI CONTROL | | |
| Secțiunea 1 Prezentare generală..... | pag. 61 | |
| Secțiunea a 2-a Investigații din oficiu..... | pag. 64 | |
| Secțiunea a 3-a Activitatea de soluționare a plângerilor..... | pag. 93 | |
| CAPITOLUL IV | | |
| ACTIVITĂȚI ÎN DOMENIUL RELAȚIILOR INTERNAȚIONALE..... | | pag. 127 |
| CAPITOLUL V | | |
| MANAGEMENTUL ECONOMIC AL AUTORITĂȚII..... | | pag. 141 |
| CAPITOLUL VI | | |
| PROPUNERI DE LEGE FERENDA..... | | pag.145 |



CAPITOLUL I

PREZENTARE GENERALĂ

Raportul de activitate pe anul 2022 al Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (denumită în continuare Autoritatea națională de supraveghere) este structurat pe șase capitole, astfel:

Capitolul I conține o prezentare sintetică a principalelor activități care se subsumează competențelor legale ale Autorității naționale de supraveghere.

În consonanță cu reglementările specifice domeniului protecției datelor cu caracter personal, activitatea instituției urmărește atingerea obiectivelor primordiale care constau în monitorizarea și controlul aplicării regulilor de prelucrare a datelor personale, în consilierea autorităților publice, a operatorilor din sectorul privat, în promovarea acțiunilor de informare a publicului larg și în asigurarea cooperării pe plan european și internațional.

În cadrul **Capitolului al II-lea** sunt cuprinse informații sintetice și relevante referitoare la activitatea de avizare a proiectelor de acte normative, de autorizare și de consiliere, precum și la cea de informare publică, în conformitate cu sarcinile și competențele stabilite de Regulamentul (UE) 2016/679, precum și cu cele stabilite de celelalte acte normative în domeniu. Această activitate s-a concretizat în emiterea avizelor asupra unui număr semnificativ de proiecte de acte normative și în elaborarea de puncte de vedere referitoare la aplicarea adecvată a normelor incidente. Opiniile s-au subsumat obiectivului de informare a publicului larg și de consiliere legislativă oferită autorităților sau instituțiilor publice competente precum și altor entități, în scopul asigurării unei aplicări unitare a principiilor de protecție a datelor personale.

Subliniem că, în anul 2022, atât persoanele fizice, cât și operatorii de date din sectorul privat și din cel public au continuat să își exprime interesul pentru aplicarea adecvată a reglementărilor din materia protecției datelor și au solicitat, în special, informații cu privire la aplicabilitatea Regulamentului (UE) 2016/679.



În secțiunea privind reprezentarea în fața instanțelor de judecată sunt prezentate cele mai semnificative litigii finalizate pe parcursul anului 2022, în care a fost parte Autoritatea națională de supraveghere, cu evidențierea soluțiilor definitive pronunțate.

Secțiunea privind informarea publică prezintă principalele modalități utilizate pentru popularizarea, în cursul anului 2022, regulilor de protecție a datelor personale, raportat la resurselor bugetare alocate.

Capitolul al III-lea constă într-o evidențiere a principalelor aspecte din activitatea de control, în privința investigațiilor din oficiu și a celor efectuate pe baza plângerilor ori sesizărilor primite, inclusiv a datelor statistice relevante.

Investigațiile efectuate din oficiu au avut ca obiect verificarea respectării prevederilor legale ca urmare, în special, a transmiterii notificărilor de încălcare a securității datelor cu caracter personal, în aplicarea art. 33 alin. (1) din Regulamentul (UE) 2016/679, precum și ca urmare a sesizărilor primite de Autoritatea națională de supraveghere.

În ceea ce privește incidentele de securitate, reieșim faptul că acestea au vizat, în principal, aspecte privind confidențialitatea, disponibilitatea sau integritatea datelor cu caracter personal afectate în special ca urmare a dezvăluirilor neautorizate; accesul neautorizat la sisteme de supraveghere video, dezvăluirea de date cu caracter personal; accesul ilegal la date cu caracter personal; divulgarea și accesul neautorizat la datele cu caracter personal ca urmare a unor atacuri informatice.

Referitor la soluționarea plângerilor și a sesizărilor, în anul 2022 au continuat să fie semnalate, în principal, aspecte referitoare la încălcarea principiilor și condițiilor de prelucrare a datelor cu caracter personal reglementate de dispozițiile art. 5 și 6 din Regulamentul (UE) 2016/679; la încălcarea drepturilor persoanelor vizate, în special a dreptului de acces al persoanei vizate, de opoziție și a dreptului la ștergerea datelor; la dezvăluirea datelor cu caracter personal fără consimțământul persoanelor vizate; la publicarea/dezvăluirea datelor cu caracter personal în mediul on-line, în special pe rețelele sociale; la prelucrarea imaginilor prin intermediul sistemelor de supraveghere video; la încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date personale prin neadaptarea de către operatori a măsurilor tehnice și organizatorice adecvate privind asigurarea securității prelucrărilor; la prelucrarea datelor cu caracter personal cu încălcarea condițiilor privind legalitatea prelucrării.



De asemenea, în cuprinsul acestui capitol, sunt evidențiate măsurile corective dispuse în urma investigațiilor efectuate, inclusiv sancțiunile aplicate, dar și o serie de exemple cu cele mai relevante cazuri investigate.

În cadrul investigațiilor efectuate în anul 2022, au fost aplicate sancțiuni contravenționale constând în amenzi în quantum total de 1.058.863 lei.

Capitolul al IV-lea prezintă activitatea de relații externe a Autorității naționale de supraveghere, prin sintetizarea diferitelor documente adoptate la nivelul Uniunii Europene, cum ar fi orientări, avize, declarații, dar și a informațiilor privind transferul datelor în temeiul regulilor corporatiste obligatorii (BCR).

Totodată, sunt expuse aspecte relevante privind cooperarea cu alte autorități de supraveghere din Uniunea Europeană în vederea asigurării asistenței reciproce, precum și informații utile referitoare la punctele de vedere emise de Autoritatea națională de supraveghere pe marginea documentelor primite.

Capitolul al V-lea conține informații privind managementul economic al instituției, respectiv creditele bugetare puse la dispoziția Autorității naționale de supraveghere și cheltuielile aferente.

Capitolul al VI-lea cuprinde propunerile de lege ferenda formulate de Autoritatea națională de supraveghere.

Astfel, acest capitol conține atât propuneri de completare a legii fundamentale, în contextul reformei constituționale, cât și de modificare a unor articole din Legea nr. 190/2018 și din Legea nr. 363/2018.

Fată de aspectele prezentate în cadrul fiecărui capitol, raportat la obiectivele Autorității naționale de supraveghere, rezultă că activitatea s-a desfășurat în condiții normale, cu toate că au fost deficiare resursele umane și financiare de care am dispus.

CAPITOLUL II

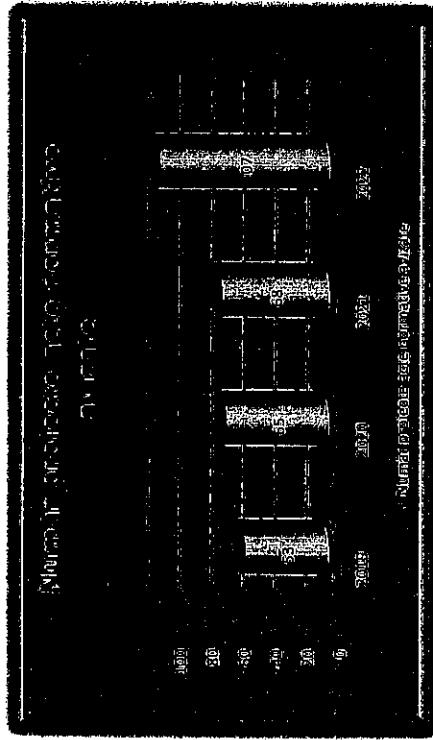
ACTIVITATEA DE AVIZARE, CONSULTARE,

REPREZENTARE ÎN FAȚA INSTANȚELOR DE JUDECATĂ ȘI INFORMARE PUBLICĂ

Secțiunea 1

Avizarea actelor normative

În anul 2022, Autoritatea națională de supraveghere a emis numeroase **avize** asupra unui număr de **107 de proiecte de acte normative** elaborate de instituții și autorități publice care implicau aspecte complexe privind prelucrarea datelor cu caracter personal, în concordanță cu atribuțiile stabilite prin prevederile art. 57 alin. (1) lit. c) din Regulamentul (UE) 2016/679.



Proiectele de acte normative au fost transmise de către unele ministere, precum, Ministerul Justiției, Ministerul Sănătății, Ministerul Transporturilor și Infrastructurii, Ministerul Dezvoltării, Lucrărilor Publice și Administrației, Ministerul Cercetării, Inovării și Digitalizării, dar și de către alte autorități sau instituții publice centrale.

De asemenea, Comisia pentru Tehnologia Informației și Comunicațiilor din cadrul Camerei Deputaților a solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la diferite propuneri legislative.

Comisia juridică, de numiri, disciplină, imunități și validări din Senat a solicitat, de asemenea, Autorității naționale de supraveghere emiterea de puncte de vedere cu privire la demersurile legislative privind unele proiecte de acte normative.

În majoritatea cazurilor, Autoritatea națională de supraveghere a apreciat că este necesară completarea sau modificarea textelor respective, efectuând o serie de observații și propuneri, prin raportare la necesitatea armonizării unor dispoziții din proiectele respective cu principiile și condițiile de prelucrare a datelor cu caracter personal.

În continuare, **prezentăm unele dintre cele mai importante proiecte de acte normative avizate:**

► **Ministerul Sănătății a supus avizării Autorității naționale de supraveghere proiectul Ordonanței de urgență a Guvernului privind stabilirea cadrului instituțional, precum și măsurile necesare pentru asigurarea aplicării directe a prevederilor Regulamentului (UE) 2017/746 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale pentru diagnostic în vitro, de abrogare a Directivei 98/79/CE și a Deciziei 2010/227/UE a Comisiei**

Autoritatea națională de supraveghere a formulat observații și propuneri în ceea ce privește textul proiectului de act normativ.

Astfel, având în vedere conținutul proiectului, prin raportare la dispozițiile Regulamentului (UE) 2016/679, s-a solicitat introducerea unui articol distinct în textul Ordonanței, referitor la faptul că orice prelucrare de date cu caracter personal realizată către entitățile prevăzute de prezenta ordonanță se realizează cu respectarea prevederilor Regulamentului (UE) 2016/679, ale Legii nr. 190/2018 privind măsurile de punere în aplicare a Regulamentului (UE) 2016/679, precum și a celorlalte reglementări specifice din domeniul protecției datelor.

Autoritatea națională de supraveghere a propus, de asemenea, completarea textului proiectului cu mențiuni referitoare la informarea persoanelor testate, raportat la drepturile persoanelor vizate prevăzute de art. 12-17 Regulamentul (UE) 2016/679, precum și



introducerea unor prevederi referitoare la obligativitatea obținerii consimțământului acestor persoane.

În consecință, s-a propus modificarea textului proiectului de Hotărâre a Guvernului, prin raportare la aspectele prezentate.

► **Comisia Juridică, de numiri, disciplină, imunități și validări din Senat a solicitat Autorității naționale de supraveghere emiterea de puncte de vedere cu privire la demersurile legislative privind proiectul de *Lege privind stabilirea cadrului organizatoric în scopul operaționalizării la nivel național a sistemului centralizat pentru determinarea statelor membre care dețin informații privind condamnările resortisanților țărilor terțe și ale apatrizilor, precum și pentru modificarea și completarea Legii nr. 290/2004 privind cazierul judiciar și cu privire la Propunerea legislativă pentru completarea Legii nr. 290 din 24 Iunie 2004 privind cazierul judiciar (republicată)***

În ceea ce privește proiectul de *Lege privind stabilirea cadrului organizatoric în scopul operaționalizării la nivel național a sistemului centralizat pentru determinarea statelor membre care dețin informații privind condamnările resortisanților țărilor terțe și ale apatrizilor, precum și pentru modificarea și completarea Legii nr. 290/2004 privind cazierul judiciar*, s-a precizat că instituția noastră a fost consultată de inițiator în procesul de avizare interministerială, a avizat actul normativ și, ca atare, susține proiectul.

Proiectul de lege creează cadrul pentru aplicarea Regulamentului (UE) 2019/816 al Parlamentului European și al Consiliului din 17 aprilie 2019 de stabilire a unui sistem centralizat pentru determinarea statelor membre care dețin informații privind condamnările resortisanților țărilor terțe și ale apatrizilor (ECRIS-TCN), destinat să completeze sistemul european de informații cu privire la cazierul judiciar și de modificare a Regulamentului (UE) 2018/1726.

Totodată, asigură transpunerea la nivel național a Directivei (UE) 2019/884 a Parlamentului European și a Consiliului din 17 aprilie 2019 de modificare a Deciziei-cadru 2009/315/JAI a Consiliului în ceea ce privește schimbul de informații privind resortisanții țărilor terțe și în ceea ce privește sistemul european de informații cu privire la cazierul judiciar (ECRIS) și de înlocuire a Deciziei 2009/316/JAI a Consiliului.



În ceea ce privește *Propunerea legislativă pentru completarea Legii nr. 290 din 24 Iunie 2004 privind cazierul judiciar (republicată)*, Autoritatea națională de supraveghere a formulat unele observații.

Referitor la depunerea online a cererilor-tip, instituția noastră a precizat că se impune stabilirea, prin proiect, de măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscurilor.

De asemenea, față de accesul online la Sistemul Național de Evidență Informatizată a Cazierului Judiciar menționat în cuprinsul proiectului, Autoritatea națională de supraveghere a precizat că aceasta implică o serie de riscuri, nefiind stabilite garanțiile necesare raportat la riscurile prelucrării pe internet a datelor cu caracter personal.

Pe de altă parte, la art. 34 din proiect, s-a apreciat că este necesară reanalizarea pct. (2.3) astfel încât proiectul să nu conțină doar o trimitere la o Hotărâre de Guvern prin care "să se stabilească procedura de acces online a persoanelor fizice (...)" la datele din Sistemul Național de Evidență Informatizată a Cazierului Judiciar, modalitatea de generare și descărcare a certificatului de cazier judiciar", întrucât rezultatul că se vor reglementa prin act subsequent prelucrări de date cu caracter personal ale persoanelor fizice.

În acest context, s-a precizat că o protecție adecvată a drepturilor persoanelor vizate este cea stabilită prin lege, așa cum a stabilit Curtea Constituțională a României în Decizia nr. 498/2018.

Totodată, față de modul de redactare a art. 34 pct. (2.3) din proiect, s-a subliniat că aceasta nu conține garanțiile prevăzute de Regulamentul (UE) 2016/679, în ceea ce privește prelucrarea datelor cu caracter personal, precum și particularizarea acestora la situațiile specifice expuse în proiect.

► **Ministerul Dezvoltării, Lucrărilor Publice și Administrației a supus avizării Autorității naționale de supraveghere proiectul de *Lege pentru aprobarea Codului amenajării teritoriului, urbanismului și construcțiilor*.**

Autoritatea națională de supraveghere a formulat observații și propuneri în ceea ce privește textul proiectului de act normativ.

Ca observație cu caracter general, s-a subliniat că trimitenle din cuprinsul proiectului privind "respectarea legislației privind protecția datelor cu caracter personal", sau la "protejarea drepturilor fundamentale ale persoanelor fizice cu privire la dreptul la viață



intimă, familială și privată”, nu sunt suficiente, fiind necesară instituirea garanțiilor prevăzute de Regulamentul (UE) 2016/679 și de celelalte reglementări legale aplicabile în domeniul protecției datelor cu caracter personal, precum și particularizarea acestora la situațiile specifice din proiect.

Totodată, s-a subliniat că, în cuprinsul proiectului este necesară precizarea datelor, respectiv a categoriilor de date cu caracter personal care sunt prelucrate în legătură cu amenajare teritoriului, urbanismului și construcțiilor, în vederea respectării principiilor legate de prelucrarea datelor, stabilite de art. 5 din Regulamentul (UE) 2016/679.

În ceea ce privește dispozițiile art. 424 alin. (4) din proiect, raportat la constituirea, organizarea și gestionarea Registrului Național al Construcțiilor, Autoritatea națională de supraveghere a subliniat că aceasta presupune, printre altele, efectuarea de prelucrări masive de date cu caracter personal care intră sub incidența Regulamentului (UE) 2016/679 și a Legii nr. 190/2018.

În acord cu cele de mai sus și raportat la prelucrările masive de date personale preconizate s-au menționat și aspectele statuate de Curtea Constituțională a României care, prin Decizia nr. 461/2014.

S-a atras atenția asupra faptului că este necesar să fie respectate prevederile art. 24, 25 și 32 din Regulamentul (UE) 2016/679.

În ceea ce privește prevederile art. 123 alin. (3) și 315 alin. (1) din proiectul de act normativ, cu privire la utilizarea “protocolului” ca bază legală a transmiterii de date între diverse entități implicate în aplicarea dispozițiilor proiectului de Cod, s-a precizat că este necesară reglementarea acestei operațiuni prin intermediul unui/unor acte administrative cu caracter normativ (de ex. ordine), în locul protocolului menționat.

Prin urmare, față de cele anterior expuse, Autoritatea națională de supraveghere a recomandat reanalizarea proiectului de act normativ sub aspectul celor prezentate anterior, astfel încât să răspundă exigențelor legislației europene și naționale în domeniul protecției datelor, precum și jurisprudenței Curții Constituționale a României.



► **Ministerul Cercetării, Inovării și Digitalizării a supus avizării Autorității naționale de supraveghere proiectul de Hotărâre privind guvernanța Platformei de Cloud Guvernamental**

Autoritatea națională de supraveghere a formulat observații și propuneri, raportate la conținutul proiectului supus atenției, astfel:

În contextul înființării, administrării și dezvoltării, la nivel național, a Platformei de Cloud Guvernamental este necesară stabilirea unor standarde, reguli, obligații necesare activităților operaționale, procedurale și tehnice de organizare și funcționare a acesteia, astfel încât prelucrările masive de date cu caracter personal care se vor efectua în cadrul acesteia să respecte prevederile exprese din Regulamentul (UE) 2016/679, precum și din celelalte acte normative aplicabile domeniului protecției datelor.

Prin urmare, ca observație cu caracter general, s-a subliniat că simpla trimitere din art. 36 lit. g) din proiect, referitoare la faptul că “aplicațiile respectă regimurile de acces la date prevăzute la nivel național și european”, precum și legislația în domeniul protecției datelor, ori trimiterea vagă sau neclară, la anumite prevederi din Regulamentul (UE) 2016/679, nu este suficientă, fiind necesară instituirea de garanții în ceea ce privește prelucrarea datelor cu caracter personal, precum și particularizarea acestora la situațiile specifice.

Autoritatea națională de supraveghere a subliniat că este necesar a se avea în vedere faptul că, la stabilirea unor standarde, reguli, obligații necesare activităților operaționale, procedurale și tehnice de organizare și funcționare a Platformei de Cloud Guvernamental elaborate de ADR, vor fi implicate și autorități și instituții publice competente în scopul prevenirii, descoperirii, cercetării, urmării penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, situație în care prelucrările de date cu caracter personal le pot fi aplicabile și alte acte normative naționale sau europene (cum ar fi Legea nr. 363/2018 ori Legea nr. 362/2018), nefiind incidente doar dispozițiile Regulamentului (UE) 2016/679.

Prin urmare s-a considerat că este necesară reanalizarea proiectului de act normativ prin raportare și la prevederile Legii nr. 190/2018, Legii nr. 363/2018, Legii nr. 506/2004, precum și ale Legii nr. 362/2018, după caz.

Față de textul proiectului s-a evidențiat că este necesară reanalizarea în vederea completării și, după caz, modificării art. 2 din proiect referitor la termenii, respectiv expresiile utilizate în conținutul acestuia, inclusiv prin raportare la definițiile din Regulamentul (UE) 2016/679.

S-a mai subliniat necesitatea reanalizării prevederilor art. 28-31 din proiect, în ceea ce privește identificarea de către USC-uri și încadrarea datelor în diferite nivele de risc asociat, în contextul în care Regulamentul (UE) 2016/679 stabilește în mod expres reguli de prelucrare (inclusiv dezvăuire) pentru anumite categorii de date cu caracter personal (de ex. datele cu caracter special ori cele referitoare la condamnări penale și infracțiuni).

Ca atare, s-a apreciat necesară reanalizarea proiectului, în întregimea acestuia, în ceea ce privește rolul și atribuțiile autorităților implicate, așa cum sunt stabilite prin proiectul de act normativ supus analizei, precum și prin Ordonanța de Urgență a Guvernului nr. 89/2022, prin raportare la art. 4 pct. 7 și pct. 8, art. 5, art. 24 și art. 32 din Regulamentul (UE) 2016/679.

În ceea ce privește efectuarea de prelucrări de date cu caracter personal, în legătură cu platforma de cloud guvernamental, cu privire la dispozițiile art. 13 alin. (1) lit. c) și 21 alin. (1) din proiect, referitor la acorduri încheiate de ADR cu USC 'cu privire la migrarea, integrarea și interconectarea în CPG', s-au precizat cele statuate de CJUE în cauza C-201/14 (Smaranda Bara și alții) în ceea ce privește baza legală a transmiterii unor date personale între diverse entități publice.

Referitor la dispozițiile art. 24 alin. (3) din proiect s-a precizat că utilizarea sintagmei "transferul datelor cu caracter personal prin intermediul platformei" creează confuzie prin raportare la dispozițiile art. 45-49 din Regulamentul (UE) 2016/679, fiind necesară reanalizarea acestora.

S-a considerat necesară completarea proiectului de act normativ prin introducerea unui nou articol care să conțină dispoziții exprese referitoare la notificarea către Autoritatea națională de supraveghere a încălcărilor de securitate de către operatorii de date implicați în prelucrările de date efectuate în platforma de cloud guvernamental.

În contextul celor de mai sus, s-a subliniat că este necesară atât respectarea termenelor exprese referitoare la notificarea încălcărilor de securitate prevăzute de art. 33 din Regulamentul (UE) 2016/679, cât și dispozițiile art. 34 din Regulamentul (UE) 2016/679

privind informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal.

De asemenea, Autoritatea națională de supraveghere a subliniat că se impune completarea proiectului de act normativ cu un nou articol care să evidențieze obligațiile referitoare la prelucrarea datelor cu caracter personal, inclusiv respectarea tuturor drepturilor persoanelor vizate, acestea să revină MCID și ADR, în calitate de operatori, în privința întregului Cloud Privat Guvernamental, iar pe de altă parte entităților găzduite să le fie stabilite obligații referitoare la sectorul ce le revine.

În legătură cu acest aspect, s-a subliniat necesitatea respectării de către operatori și a prevederilor art. 24, art. 25 și art. 32 din Regulamentul (UE) și, ca atare, s-a recomandat reanalizarea Platformei proiectate din perspectiva acestor exigențe.

Cu privire la art. 38 din proiect s-a subliniat că acesta conține dispoziții contradictorii, care generează confuzii sub aspectul obligațiilor avute de operatorii de date, respectiv de împotrimității operatorilor, raportat la responsabilitatea operatorilor de date în a-și stabili, de exemplu, propriile măsuri tehnice și organizatorice referitoare la securitatea datelor cu caracter personal prelucrate.

În ceea ce privește interconectarea, așa cum este prevăzută de art. 21 și art. 24 din proiect, raportat la condițiile de legitimitate și principiile prelucrării datelor cu caracter personal, s-a subliniat că din proiectul de act normativ nu rezultă că prelucrările care se estimează a fi efectuate în platforma de cloud guvernamental în contextul interconectării unor sisteme informatice aparținând unor diverse entități publice ce dețin/gestionează sisteme informatice pentru prelucrări proprii de date cu caracter personal sunt în concordanță cu prevederile Regulamentului (UE) 2016/679, în special cu cele ale art. 5 și art. 6 din acest act normativ.

Totodată, cu privire la interconectarea mai multor baze de date s-a atras atenția asupra faptului că entitățile ce urmează să realizeze această interconectare prelucrează fiecare în parte date cu caracter personal în scopuri distincte, iar prin acest proiect nu se stabilește clar dacă se preconizează dublarea bazelor de date enumerate sau transferarea acestora către cloud-urile furnizate de entitățile private (art. 24 din proiect), ceea ce ridică problema respectării de acest proiect a actelor normative existente.

Față de toate cele de mai sus, în legătură cu prelucrările de date cu caracter personal efectuate în contextul Platformei de Cloud Guvernamental, raportat la condițiile de



legitimitate și principiile prelucrării datelor cu caracter personal, a rezultat necesitatea reanalizării și modificării substanțiale a proiectului de act normativ, astfel încât să răspundă exigențelor legislației europene și naționale în domeniul protecției datelor, precum și jurisprudenței Curții Constituționale a României.

► **Ministerul Sănătății a supus avizării Autorității naționale de supraveghere proiectul de modificare a art. V din OUG nr. 180/2020 pentru modificarea și completarea Legii nr. 136/2020 privind instituirea unor măsuri în domeniul sănătății publice în situații de risc epidemiologic și biologic, a Ordonanței de urgență a Guvernului nr. 158/2005 privind concediile și indemnizațiile de asigurări sociale de sănătate, precum și pentru stabilirea unor măsuri cu privire la acordarea concediilor medicale**

Autoritatea națională de supraveghere a formulat observații și propuneri, astfel: în ceea ce privește datele prelucrate în sistemul SEGIS-Forms, raportat la alin. 2 din proiect, s-a subliniat că este necesară stabilirea clară a tuturor scopurilor de prelucrare a datelor cu caracter personal, prin raportare la principiul necesității, prevăzut de art. 5 alin. (1) lit. c) din Regulamentul (UE) 2016/679.

În ceea ce privește păstrarea datelor colectate în aplicația informatică Corona-Forms, s-a precizat că este necesară reanalizarea dispozițiilor alin.1 din proiect, prin raportare la art. 5 alin. (1) lit. e) din Regulamentul (UE) 2016/679.

În același timp, cu referire la alin. (2) din proiect, Autoritatea națională de supraveghere a considerat că sintagma "o varietate de servicii" este vagă și, prin urmare, este necesară clarificarea și reformularea textului.

În ceea ce privește sistemul SEGIS-Forms care permite "interconectarea registrelor din sănătate" (alin. 2 lit. a) IV. din proiect) și "integrarea altor platforme de e-sănătate/aplicații informatice de la nivel național sau european" (alin. 2 lit. e) din proiect), s-a subliniat că aceasta presupune, printre altele, efectuarea de prelucrări masive de date cu caracter personal care intră sub incidența Regulamentului (UE) 2016/679, a Legii nr. 190/2018, precum și a celorlalte acte normative aplicabile domeniului protecției datelor cu caracter personal.

Prin urmare, ca observație cu caracter general, s-a precizat că este necesar a fi menționat distinct, în cuprinsul proiectului, că prelucrările de date ce urmează a se realiza



prin SEGIS-Forms sunt supuse reglementărilor Regulamentului (UE) 2016/679, Legii nr. 190/2018 și a celorlalte acte normative aplicabile domeniului protecției datelor cu caracter personal.

Mai mult, s-a subliniat că simpla trimitere la faptul că cererile referitoare la datele prelucrate în SEGIS-Forms și la exercitarea drepturilor persoanelor vizate, așa cum sunt prevăzute în art. 13-22 din Regulamentul (UE) 2016/679 făcută în cuprinsul alin. (3) din proiect, nu este suficientă, fiind necesară instituirea de garanții, precum și particularizarea acestora la situațiile specifice din proiect.

Legat de cele de mai sus s-a precizat că este necesară clarificarea aspectelor referitoare la dreptul persoanelor vizate la ștergerea datelor prevăzut de art. 17 din Regulamentul (UE) 2016/679, așa cum este reglementat în alin. (6), în sensul că exercitarea acestui drept este restricționată numai în situațiile prevăzute de art. 17 alin. (3).

În același timp, s-a considerat că este necesară menționarea tuturor datelor/categoriilor de date cu caracter personal care urmează a fi prelucrate prin SEGIS-Forms (în sensul definiției din art. 4 pct. 2), raportat la fiecare dintre scopurile prelucrărilor de date ce urmează a fi efectuate în SEGIS-Forms, având în vedere implicațiile creării sistemului ce permite și interconectarea și interoperabilitate cu alte sisteme informatice, platforme hardware și software, conform alin. (7) din proiect și deci, implicit, posibilele afectări ale dreptului la protecția datelor a mai multor persoane vizate, cu atât mai mult cu cât, cea mai mare parte dintre aceste date sunt cele privind sănătatea, a căror prelucrare comportă riscuri deosebite pentru drepturile și libertățile persoanelor vizate.

Autoritatea națională de supraveghere a subliniat că precizarea datelor, respectiv a categoriilor de date cu caracter personal care sunt prelucrate prin intermediul SEGIS-Forms, este necesară în vederea respectării principiilor legate de prelucrarea datelor, stabilite de art. 5 din Regulamentul (UE) 2016/679, în vederea respectării prevederilor Legii nr. 24/2000, cu modificările și completările ulterioare, raportat și la jurisprudența constantă a Curții Constituționale a României.

În acord cu cele de mai sus și raportat la prelucrările masive de date personale preconizate (din sisteme informatice naționale, registre naționale de evidență, platforme, respectiv din baze de date naționale ale multor autorități și instituții publice din România), s-au menționat aspectele statuate prin Decizia nr. 461/2014 de Curtea Constituțională a României prin care a motivat că actul normativ analizat nu respectă, în integralitatea sa,

condițiile impuse de principiul proporționalității, nu oferă garanții care să asigure confidențialitatea datelor cu caracter personal, aducând atingere însăși esenței drepturilor fundamentale referitoare la viața intimă, familială și privată, precum și libertății de exprimare.

Pe de altă parte, s-a subliniat că este necesară menționarea, în cuprinsul proiectului, dacă SEGIS-Forms permite realizarea de schimburi de date cu caracter personal și în măsura în care acestea sunt permise, stabilirea concretă a entităților care prelucrează date cu caracter personal (altale decât Ministerul Sănătății și Împundernicul acestuia, respectiv Serviciul de Telecomunicații Speciale) în contextul interconectării între sistemele informatice ale autorităților/instituțiilor publice și dacă este cazul, raportat la dispozițiile alin. 2 lit. a) IV. și lit. e), respectiv alin. 7 din proiect, menționarea altor participanți la schimbul de date, alții decât o instituție sau autoritate publică, astfel încât să nu se încalce prevederile art. 6 alin. (4) din Regulamentul (UE) 2016/679.

Raportat la dispozițiile alin. (4) și (5) din proiect, Autoritatea națională de supraveghere a considerat că este necesar să se stabilească clar accesul, cât și limitele accesului entităților participante la SEGIS-Forms, respectiv a persoanelor aflate sub autoritatea acestora, astfel încât să fie respectate prevederile art. 24, art. 25 și art. 32 din Regulamentul (UE) 2016/679.

În ceea ce privește prevederile alin. (7) din proiect, cu referire la "acordul de colaborare încheiat între Ministerul Sănătății, administratorul tehnic al aplicației sau sistemului informatic în cauză și instituția sau autoritatea publică care deține seturile de date necesare" s-a atras atenția în ceea ce privește baza legală a transmiterii unor date personale între diverse entități publice că, așa cum a statuat și Curtea de Justiție a Uniunii Europene în cauza C-201/14 (Smaranda Bara și alții).

Prin urmare, față de cele anterioare expuse, Autoritatea națională de supraveghere a recomandat reanalizarea proiectului de act normativ, sub aspectul celor prezentate anterior, astfel încât să răspundă exigențelor legislației europene și naționale în domeniul protecției datelor, precum și jurisprudenței Curții Constituționale a României.

► **Comisia pentru Tehnologia Informației și Comunicațiilor din cadrul Camerei Deputaților a solicitat Autorității naționale de supraveghere exprimarea unui punct de vedere cu privire la propunerea legislativă referitoare la *Legea interoperabilității*.**

Autoritatea națională de supraveghere a formulat observații și propuneri.

Interconectarea sistemelor informatice ale instituțiilor și autorităților publice în vederea realizării unui schimb de date între aceste entități, presupune, printre altele, efectuarea de prelucrări masive de date cu caracter personal care sunt reglementate în mod expres prin Regulamentul (UE) 2016/679, fiind necesară instituirea garanțiilor prevăzute de acest act normativ în ceea ce privește prelucrarea datelor cu caracter personal, precum și particularizarea acestora la situațiile specifice din proiect.

Totodată, întrucât pentru asemenea situație prezentată în propunere nu sunt incidente doar prevederile Regulamentului (UE) nr. 2016/679, Autoritatea națională de supraveghere a considerat că este necesară reanalizarea propunerii de act normativ prin raportare și la prevederile Legii nr. 190/2018, ale Legii nr. 363/2018 și, după caz, ale Legii nr. 506/2004.

Față de textul propunerii s-a considerat că este necesară reanalizarea, completarea și, după caz, modificarea art. 3 din proiect referitor la termenii, respectiv expresiile utilizate în conținutul proiectului de act normativ, inclusiv prin raportare la definițiile din Regulamentul (UE) 2016/679.

În ceea ce privește efectuarea de prelucrări de date cu caracter personal, așa cum sunt acestea definite în art. 4 pct. 1 din Regulamentul (UE) 2016/679, în legătură cu implementarea, operaționalizarea și funcționarea platformei naționale de interoperabilitate, s-au precizat următoarele aspecte care trebuie avute în vedere în cuprinsul proiectului de act normativ:

- Stabilirea concretă a entităților care prelucrează date cu caracter personal în contextul interconectării între sistemele informatice ale autorităților/instituțiilor publice, participanți la schimbul de date, alții decât o instituție sau autoritate publică, respectiv utilizatori de date așa cum sunt definiți în art. 3 lit. n) din propunere, astfel încât să nu se încalce prevederile art. 6 alin. (4) din Regulamentul (UE) 2016/679.

- Stabilirea concretă a calității și a obligațiilor autorităților și instituțiilor publice care prelucrează date cu caracter personal în cadrul platformei naționale de interoperabilitate,



prin raportare la definițiile din art. 4 pct. 7, pct. 8, pct. 9 și pct. 10 din Regulamentul (UE) 2016/679. În acest sens, s-a precizat că este necesară reanalizarea art. 8 alin. (4) și (7), art. 9-13, precum și art. 14-19 din propunere.

- includerea unor prevederi legale specifice în aplicarea regulilor de protecția datelor prevăzute de Regulamentul (UE) 2016/679, sens în care s-a considerat că utilizarea sintagmei "în conformitate cu legislația privind protecția datelor cu caracter personal", a sintagmei "cu respectarea standardelor Regulamentului (UE) 2016/679" ori a sintagmei "standardele adecvate prelucrării datelor" în proiect, nu sunt nici suficiente, nici clare sau previzibile.

În același timp, s-a considerat că este necesară introducerea în propunerea de act normativ a unor dispoziții prin care să fie precizate datele, respectiv categoriile de date cu caracter personal care vor face obiectul schimbului de date prin intermediul platformei naționale de interoperabilitate, în vederea respectării principiilor legate de prelucrarea datelor.

În contextul celor de mai sus, s-a subliniat că Autorității pentru Digitalizarea României (ADR), entitatea care administrează, conform art. 9 alin. (2) din propunere, platforma națională de interoperabilitate, îi revin toate obligațiile stabilite în sarcina unui operator de date cu caracter personal, prin raportare la definiția acestuia din art. 4 pct. 7 din Regulamentul (UE) 2016/679.

- Referitor la dispozițiile art. 10 din propunere, s-a arătat că este necesar să se clarifice și să menționeze în mod expres care este autoritatea competentă la care se face referire, în contextul în care, în România, Autoritatea națională de supraveghere este autoritatea care exercită competențele care îi sunt conferite în conformitate cu Regulamentul (UE) 2016/679, inclusiv sub aspectul exercitării competențelor de investigare, respectiv de monitorizare și de asigurare a aplicării acestui act normativ.

Aceeași observație a fost formulată și cu referire la clarificarea aspectelor privind "autoritatea competentă" și în legătură cu prevederile art. 17 alin. (1) lit. e) și art. 20 alin. (2) din propunere.

- S-a propus reanalizarea dispozițiilor art. 17 alin. (1) lit. f) prin raportare la prevederile art. 37, art. 38 și art. 39 din Regulamentul (UE) 2016/679, care conțin prevederi exprese cu privire la desemnarea, funcția și sarcinile responsabilului cu protecția datelor.

- În ceea ce privește interconectarea sistemelor informatice ale instituțiilor/autorităților publice participante la platforma națională de interoperabilitate, s-a precizat că este necesară



stabilirea modalităților de acces și a limitelor accesului entităților participante la schimbul de date, respectiv a utilizatorilor platformei (în sensul art. 3 lit. n din propunere), astfel încât să fie respectate prevederile art. 24, art. 25 și art. 32 din Regulamentul (UE) 2016/679.

- Totodată, cu privire la interconectarea a diverse baze de date în contextul creării platformei naționale de interoperabilitate, s-a atras atenția asupra faptului că entitățile ce urmează să participe la acesta prelucrează fiecare în parte date cu caracter personal în scopuri distincte, iar prin acest proiect nu se stabilește clar dacă se preconizează dublarea bazelor de date enumerate sau transferarea acestora către ADR, ceea ce ridică problema corelării acestui proiect cu actele normative existente.

Prin urmare, este necesar ca, la crearea platformei, să fie luate în considerare prevederile art. 6 alin. (4) din Regulamentul (UE) 2016/679, care instituie exigența compatibilității între scopul inițial al prelucrării și cel ulterior și care trebuie să se reflecte în dreptul intern aplicabil operatorului, pentru a se institui garanții adecvate protejării drepturilor persoanelor vizate.

În consecință, Autoritatea națională de supraveghere a considerat că este necesară reanalizarea integrală și modificarea substanțială a propunerii legislative referitoare la Legea interoperabilității.

► **Agenția Națională a Funcționarilor Publici a solicitat Autorității naționale de supraveghere exprimarea unui punct de vedere cu privire la *proiectul de Ordonanță de urgență a Guvernului pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 57/2019 privind Codul Administrativ.***

Autoritatea națională de supraveghere a recomandat modificarea textului proiectului în sensul următoarelor observații și propuneri:

Față de prevederile punctului 6 din proiect, având în vedere prevederile art. 411 alin. (4) din OUG nr. 57/2019 care prevede obligația autorităților și instituțiilor publice de a introduce în sistemele informatice date privind personalul propriu, s-a propus reformularea alin. (1¹) al art. 410. De asemenea, la punctul 8 din proiect s-a propus eliminarea din cadrul art. 411 alin. (2), teza a doua, a sintagmei „precum și direct”, raportat la prevederile alin. (4) referitoare la obligația autorităților și instituțiilor publice de a introduce în sistemele informatice date privind personalul propriu, întrucât prin accesarea directă de către Agenția Națională a Funcționarilor Publici a bazelor de date ale instituțiilor și autorităților publice s-ar

aduce atingere dreptului la protecția datelor ale personalului bugetar plătit din fonduri publice.

La același punct 8 din proiect, privind modificarea alin. (5) al art. 411, s-a apreciat că interconectarea sistemelor informatice prevăzute la acest alineat vine în contradicție cu prevederile alin. (4) din OUG nr. 57/2019, implicând riscuri în asigurarea protecției datelor întrucât se efectuează o prelucrare masivă de date personale fără garanții, raportat la scopul prelucrării (întocmirea, actualizarea și administrarea evidenței personalului bugetar plătit din fonduri publice).

La punctul 9 din proiect s-a propus reanalizarea alin. (8²) al art. 411, întrucât nu rezultă și necesitatea accesării tuturor datelor personale din Registrul național de evidență a persoanelor, administrat de Direcția pentru Evidența Persoanelor și Administrarea Bazelor de date din cadrul Ministerului Afacerilor Interne, având în vedere că datele sunt furnizate chiar de autoritățile și instituțiile publice deținătoare.

Față de prevederile art. 113 alin. (10) din Anexa 2 la proiect, s-a propus introducerea unui termen limită de stocare a datelor, având în vedere că din textul articolului rezultă că datele sunt prelucrate pe o perioadă nedeterminată, pentru respectarea prevederilor art. 5 din Regulamentul (UE) 2016/679, referitor la principiile de prelucrare, în special a principiului limitării legate de stocare și a principiul responsabilității.

În ceea ce privește înregistrarea audio-video a probelor de concurs din proiectul-pilot prevăzută la art. 113 din Anexa 2 la proiect, s-a subliniat că este necesar să se stabilească garanțiile prevăzute de Regulamentul (UE) 2016/679, în special cele privind informarea persoanelor vizate (art. 13; art.14), punerea în aplicare de măsuri de asigurare a securității prelucrărilor (art. 24 și art. 32), asigurarea respectării drepturilor persoanelor vizate.

► **Ministerul Justiției a solicitat Autorității naționale de supraveghere exprimarea unui punct de vedere asupra proiectului de Hotărâre a Guvernului pentru aprobarea Regulamentului privind organizarea și funcționarea Registrului Național de Publicitate Mobilă**

Față de textul proiectului sus-menționat, Autoritatea națională de supraveghere a propus introducerea unui nou articol în textul Hotărârii de Guvern referitor la faptul că toate entitățile menționate în Hotărârea de Guvern prelucreează date cu caracter personal cu

respectarea Regulamentului (UE) 2016/679, precum și a celorlalte acte normative incidente din domeniul protecției datelor personale.

În plus, referitor la mențunerea de la art. 4 lit. a) și c) privind "datele de identificare și contact", Autoritatea națională de supraveghere a propus identificarea și menționarea expresă a datelor care urmează a fi publicate.

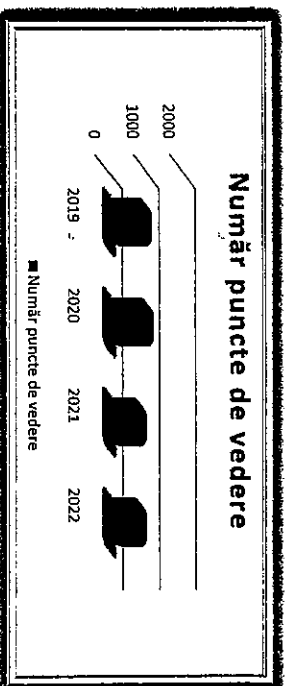
În ceea ce privește "adresa la care operatorii confirmă primirea corespondenței" menționată la art. 4 lit. b) din proiectul actului normativ în discuție, raportat la definițiile art. 1 alin. (1) lit. b) și c) și ale art. 5 alin. (2) lit. i) din Legea nr. 297/2018 privind publicitatea mobilă, republicată, la principiul proporționalității menționat de art. 5 alin. (1) lit. c) din Regulamentul (UE) 2016/679, s-a recomandat să se analizeze necesitatea acestei prelucrări.

Secțiunea a 2 – a:

Puncte de vedere privind diverse chestiuni de protecția datelor

Pe parcursul anului 2022 a fost adresat Autorității naționale de supraveghere un număr de **948 solicitări de emitere puncte de vedere** privind diverse aspecte referitoare la modalitatea de interpretare și aplicare a Regulamentului (UE) 2016/679, de către operatorii și împuterniciții acestora, din domeniul public și privat, de către alte entități, precum și de către persoane fizice.

Observăm în acest an menținerea la un nivel ridicat al numărului de solicitări, ceea ce ilustrează interesul constant al operatorilor și împuterniciților în asigurarea respectării regulilor de prelucrare a datelor personale instituite de Regulamentul (UE) 2016/679 și de legislația națională conexă.



■ **Prezentăm în continuare unele dintre cazurile semnificative supuse atenției Autorității naționale de supraveghere, astfel:**

◆ ***Prelucrarea datelor personale de către autorități/instituții publice prin intermediul telefonului personal sau prin aplicația WhatsApp***

Unele autorități și instituții publice (inclusiv poliții locale) au solicitat Autorității naționale de supraveghere opinia privind utilizarea mijloacelor de comunicare între aceste autorități/instituții atât cu cetățenii, cât și în cadrul acestora, între angajați, prin intermediul telefonului personal sau prin aplicația WhatsApp.

Având în vedere principiul responsabilității operatorilor (în speță, autorități/instituții publice), Autoritatea națională de supraveghere a subliniat că prelucrarea datelor fără luarea și respectarea măsurilor tehnice și organizatorice adecvate riscului prelucrării poate aduce o atingere gravă dreptului la viață privată și la protecția datelor persoanelor fizice, prin raportare la principiile de prelucrare, în special al legalității și al asigurării confidențialității și securității prelucrării datelor.

Sub aspectul măsurilor pe care operatorul trebuie să le ia pentru protejarea datelor personale înregistrate în sistemele sale de evidență, este necesar a se avea în vedere considerentele (39), (83) și (84) din Regulamentul (UE) 2016/679.

De asemenea, art. 24 și art. 32 din Regulamentul (UE) 2016/679 stabilesc anumite măsuri tehnice și organizatorice adecvate, revenind operatorului responsabilitatea punerii în aplicare a acestora, pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu acest regulament.

Prin urmare, având în vedere natura datelor prelucrate de către o instituție publică, este necesară respectarea obligațiilor stabilite de prevederile legale din Regulamentul (UE) 2016/679, în special a măsurilor privind confidențialitatea și securitatea datelor.

Ca atare, la evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod. Măsurile au în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării.

Față de cele de mai sus, rezultă că instituțiile publice, în calitate de operatori, au obligația de a pune în aplicare măsurile tehnice și organizatorice adecvate care, dacă este necesar, se revizuesc și se actualizează, pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu Regulamentul (UE) 2016/679.

În acest context, s-a precizat că, raportat la stabilirea mijloacelor de comunicare cu alte autorități și instituții publice, prelucrarea datelor ar trebui să se subsumeze îndeplinirii unei obligații legale ce revine operatorului, potrivit art. 6 alin. (1) lit. c) din Regulamentul (UE) 2016/679.

De asemenea, potrivit art. 29 din Regulamentul (UE) 2016/679, orice persoană care acționează sub autoritatea operatorului care are acces la date cu caracter personal (de ex. angajații) nu le prelucreează decât la cererea operatorului, cu excepția cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru.

În acest context, s-a subliniat faptul că, raportat la asigurarea conformității operațiunilor de prelucrare de către WhatsApp Irlanda, această companie a fost supusă investigației Autorității naționale de supraveghere irlandeze, constatându-se încălcarea principiului transparenței consacrat de articolul 5 alin. (1) lit. a) din Regulamentul (UE) 2016/679 și, implicit, a dreptului la informare a persoanelor vizate situate pe teritoriul mai multor state membre, stabilindu-se o sancțiune cu amendă semnificativă în acest sens (225 mil. Euro). Totodată, din aceeași investigație, a rezultat faptul că „WhatsApp face schimb de informații cu companiile Facebook”, iar pentru evitarea unor cazuri similare celui în care a fost implicat Facebook (Cambridge Analytica) este necesară asigurarea unei protecții reale a datelor persoanelor fizice, prin adoptarea măsurilor adecvate.

Ca atare, s-a comunicat că modalitatea de comunicare a datelor aleasă de către unele instituții publice în îndeplinirea atribuțiilor legale, respectiv prin intermediul telefonului personal sau prin aplicația WhatsApp, ridică problema conformității prelucrării sub aspectul legalității și proporționalității prelucrării, prevăzute de art. 5 și 6 din Regulamentul (UE) 2016/679.

◆ ***Prelucrarea datelor personale în contextul relațiilor de muncă***

O persoană fizică a solicitat punctul de vedere al Autorității cu privire la respectarea regulilor de prelucrare în contextul relațiilor de muncă.

S-a precizat faptul că Regulamentul (UE) 2016/679 stabilește că prelucrarea datelor cu caracter personal, inclusiv sub aspectul dezvăluirii acestora, se realizează la consimțământul persoanei vizate sau în alte condiții legale în care nu se solicită consimțământul, prevăzute de art. 6, art. 9 și art. 10, în funcție de natura datelor și categoriilor de date colectate și prelucrate.

În ceea ce privește consimțământul angajaților, Autoritatea națională de supraveghere a subliniat că, în Avizul nr. 2/2017 privind prelucrarea datelor la locul de muncă, Grupul de Lucru art. 29 (în prezent Comitetul European pentru Protecția Datelor) a semnalat următoarele:

“Angajații nu sunt aproape niciodată în măsură să își exprime, să refuze sau să își revoce în mod liber consimțământul, având în vedere dependența care rezultă din relația dintre angajator și angajat. Având în vedere dezzechilibrul de puteri, angajații își pot da consimțământul liber numai în situații excepționale, atunci când nu există deloc consecințe legate de acceptarea sau respingerea unei oferte.”

În ceea ce privește sistemele de monitorizare a angajaților la locul de muncă, Autoritatea națională de supraveghere a făcut trimitere și la prevederile art. 5 din Legea nr. 190/2018. Astfel, sub aspectul uneia din condițiile de legalitate a prelucrării - interesul legitim, prevăzut de art. 6 alin. (1) lit. f) din Regulamentul (UE) 2016/679, acesta se coroborează cu considerentul (47) al Regulamentului (UE) 2016/679 și art. 5 din Legea nr. 190/2018.

În acest context s-a precizat faptul că, pentru a demonstra existența interesului legitim este necesară realizarea testului comparativ. Ulterior realizării testului comparativ și asumării de operator a faptului că temeiul legal al prelucrării datelor va fi interesul legitim, se realizează prelucrarea acestora pe baza art. 6 alin. (1) lit. f) din Regulamentul (UE) 2016/679, cu îndeplinirea tuturor condițiilor prevăzute de art. 5 din Legea nr. 190/2018.

În plus, s-a precizat că în ceea ce privește prelucrarea datelor în mod transparent față de persoana vizată (indiferent de temeiul legal al prelucrării), art. 12 din Regulamentul (UE) 2016/679 prevede că operatorul la măsură adecvate pentru a furniza persoanei vizate orice informații menționate la articolele 13 și 14 și orice comunicații în temeiul articolelor 15-22 și 34 referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu.

Artfel, art. 13 din Regulamentul (UE) 2016/679 prevede că în cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, operatorul, în momentul obținerii datelor, furnizează persoanei vizate informațiile prevăzute de aceste dispoziții legale.

De asemenea, în Avizul nr. 2/2017 privind prelucrarea datelor la locul de muncă se mai menționează: “Faptul că un angajator deține proprietatea asupra mijloacelor electronice nu exclude dreptul angajaților la confidențialitatea comunicațiilor lor, a datelor de localizare aferente și a corespondenței lor.”

Prin urmare, Autoritatea națională de supraveghere a subliniat că, în contextul prelucrării datelor personale ale angajaților, anterior derulării relațiilor de muncă, angajatorii (operatorii) au obligația de a asigura informarea salariaților potrivit art. 13 și art. 14 din Regulamentul (UE) 2016/679, după cum datele sunt obținute în mod direct sau indirect, context în care angajațiiiau cunoștință de scopurile și temeiul juridic al prelucrării, precum și de eventuala prelucrare ulterioară a datelor cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate.

În ceea ce privește măsurile de securitate ce se impun a fi adoptate de către operator (angajator), s-a precizat că art. 32 din Regulamentul (UE) 2016/679 stabilește o serie de aspecte pe care operatorul trebuie să le urmărească în contextul implementării măsurilor tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului pe care o are prelucrarea pentru drepturile și libertățile persoanelor fizice.

În acest context, Autoritatea națională de supraveghere a subliniat faptul că, potrivit principiului responsabilității (art. 24), operatorul trebuie să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu Regulamentul(UE) 2016/679.

Raportat la arhitectura unui sistem informatic utilizat de angajator, s-a precizat că operatorul trebuie să asigure, în conformitate cu art. 25 din Regulamentul (UE) 2016/679, protecția datelor începând cu momentul conceperii și în mod implicit (principiile privacy by design și privacy by default).

Față de cele de mai sus, în contextul prelucrării datelor personale ale angajaților, Autoritatea națională de supraveghere a subliniat că este necesară analiza, de către angajator, prin raportare la reglementările legale specifice din domeniul său de activitate, a temeiului legal al prelucrării în conformitate cu dispozițiile precizate, cu respectarea



principiilor de prelucrare a datelor stabilite în art. 5 din Regulamentul (UE) 2016/679, în special al legalității, transparenței, limitării legate de scop și al reducerii la minimum a datelor, precum și a măsurilor de securitate, în conformitate cu dispozițiile Regulamentului (UE) 2016/679 și jurisprudența relevantă.

➔ ***Prelucrarea de date biometrice în vederea accesului într-o sală de fitness***

O persoană fizică a solicitat punctul de vedere al Autorității cu privire la respectarea Regulamentului (UE) 2016/679, în contextul prelucrării de date biometrice în scopul accesului într-o sală de fitness.

În ceea ce privește datele biometrice, Autoritatea națională de supraveghere a subliniat că art. 4 pct. 14 din Regulamentul (UE) 2016/679 definește aceste date ca fiind "date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice".

În acest context, s-a precizat că, în Avizul 4/2007 privind conceptul de date cu caracter personal, Comitetul European pentru Protecția Datelor arată că: "Aceste date - datele biometrice pot fi definite ca proprietăți biologice, caracteristici fiziologice, trăsături vitale sau acțiuni repetate, atât trăsăturile cât și/sau acțiunile fiind caracteristice persoanei și fiind măsurabile, chiar dacă modelele utilizate în practică pentru măsurarea din punct de vedere tehnic a acestora implică un anumit grad de probabilitate. Exemple tipice ale unor asemenea date biometrice sunt amprentele digitale, modelele retinei, structura feței, vocile, precum și geometria mâinii, modelele sanguine sau chiar unele aptitudini înrădăcinate sau alte trăsături comportamentale (precum semnătura de mână, felul de a se mișca, în special felul de a merge sau de a vorbi etc.)".

Corelat cu cele de mai sus, în Avizul 3/2012 privind progresele înregistrate de tehnologiile biometrice, Comitetul european pentru protecția datelor menționează că "există două categorii principale de tehnici biometrice", unele dintre acestea referindu-se la "tehnicile bazate pe caracteristici fizice și fiziologice, care măsoară caracteristicile fizice și fiziologice ale unei persoane și care includ: verificarea amprentelor digitale, analiza imaginii degetului, recunoașterea irisului, analiza retinei, recunoașterea facială, modelul conturului mâinii,



recunoașterea formei urechilor, detectarea mirosului corporal, recunoașterea vocală, analiza tiparului ADN, analiza porilor sudoripari etc."

Referitor la prelucrarea datelor biometrice, s-a precizat că aceasta este supusă condițiilor art. 9, iar potrivit art. 9 alin. (2) lit. a) din Regulamentul (UE) 2016/679, datele biometrice pot fi prelucrate dacă persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date pentru unul sau mai multe scopuri specifice.

Referitor la valabilitatea consimțământului angajaților, s-a precizat că în Ghidul nr. 05/2020 privind consimțământul în temeiul Regulamentului (UE) 2016/679, emis de Comitetul European pentru Protecția Datelor, se menționează faptul că "Un dezechilibru de putere apare, de asemenea, în contextul relațiilor de muncă. Având în vedere dependența care rezultă din relația dintre angajator și angajat, este puțin probabil ca persoana vizată să poată refuza să-și acorde consimțământul față de angajatorul său pentru prelucrarea datelor fără a se confrunta cu temerea sau cu riscul real de consecințe negative ca urmare a unui refuz. Este puțin probabil ca un angajat să poată răspunde în mod liber la o cerere de consimțământ din partea angajatorului său. (...)Având în vedere dezechilibrul de putere dintre un angajator și membrii personalului său, angajații își pot da consimțământul în mod liber numai în circumstanțe excepționale, și anume atunci când nu va exista nicio consecință negativă, indiferent dacă aceștia consimt sau nu."

În ceea ce privește proporționalitatea instituirii unei asemenea măsuri, s-a mai arătat că Grupul de Lucru Art. 29 (în prezent Comitetul european pentru protecția datelor) precizează, în Avizul 3/2012 privind progresele înregistrate de tehnologiile biometrice, faptul că: "Utilizarea biometriei ridică problema proporționalității fiecărei categorii de date prelucrate în lumina scopului în care sunt prelucrate acestea. Având în vedere faptul că datele biometrice pot fi utilizate numai dacă sunt adecvate, relevante și neexcesive, trebuie să se evalueze cu exactitate necesitatea și proporționalitatea datelor prelucrate și să se analizeze dacă scopul urmărit ar putea fi atins într-un mod mai puțin intruziv."

În contextul celor menționate și al necesității asigurării unei protecții eficiente a dreptului la viață privată și la protecția datelor personale, raportat la principiul proporționalității prelucrării, s-a precizat că instituția noastră a sancționat în mai multe rânduri prelucrarea de către operatori a datelor biometrice ale angajaților proprii considerând aceasta ca fiind excesivă raportat la scopul urmărit, respectiv pontaj (a se vedea spre



exemplificare, comunicatul de presa din 2 Iunie 2016, accesibil la adresa https://www.dataprotection.ro/?page=sanctiuni_mai&lang=ro).

Față de cele de mai sus, având în vedere natura sensibilă a datelor care necesită protecție, raportat la principiul legalității și proporționalității instituite de art. 5 și art. 9 din Regulamentul (UE) 2016/679, la condițiile de valabilitate a consimțământului prevăzute de art. 7 din același regulament, precum și aplicabilitatea acestora în relația angajat - angajator, s-a precizat că situația prezentată nu se subsumează cerințelor de legalitate, necesitate și proporționalitate a prelucrării datelor biometrice și nu se justifică necesitatea și proporționalitatea prelucrării de date biometrice, prin raportare la scopul urmărit (acces în incinta clubului de fitness), fiind necesară alegerea unei alte soluții mai puțin intruzive pentru atingerea respectivului scop, care nu implică prelucrarea datelor biometrice ale persoanelor vizate.

♦ **Prelucrarea de date personale ale clienților cu care instituțiile financiare**

nebanzare au negociat tranzacții, chiar dacă respectivele tranzacții nu s-au finalizat

O persoană fizică a solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la temeiul prelucrării datelor cu caracter personal ale clienților cu care instituțiile financiare nebanzare au negociat tranzacții, chiar dacă respectivele tranzacții nu s-au finalizat.

În ceea ce privește legalitatea prelucrărilor, Autoritatea națională de supraveghere a subliniat faptul că Regulamentul (UE) 2016/679 prevede că prelucrarea datelor cu caracter personal se realizează cu consimțământul persoanei vizate sau în celelalte condiții prevăzute de art. 6, art. 9 și art. 10, în funcție de natura datelor și categoriilor de date colectate și prelucrate.

Față de cele de mai sus, raportat la conținutul adresei, s-a menționat că art. 8 din Legea nr. 93/2009 privind instituțiile financiare nebanzare prevede că "instituțiile financiare nebanzare pot prelucra date cu caracter personal în conformitate cu prevederile Legii nr. 677/2001, cu modificările și completările ulterioare."

Pe de altă parte, potrivit art. 2 lit. r) din Legea nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative, cu modificările și completările ulterioare, "client/clientelă



înseamnă orice persoană fizică, juridică sau entitate fără personalitate juridică cu care entitățile raportoare desfășoară relații de afaceri ori cu care desfășoară alte operațiuni cu caracter permanent sau ocazional. Se consideră client al unei entități raportoare orice persoană cu care, în desfășurarea activităților sale, entitatea raportoare a negociat o tranzacție, chiar dacă respectiva tranzacție nu s-a finalizat, precum și orice persoană care beneficiază sau a beneficiat, în trecut, de serviciile unei entități raportoare".

Art. 21 alin. (1) din Legea nr. 129/2019 prevede:

"(1) Entitățile raportoare, atunci când aplică măsurile de cunoaștere a clientelei, au obligația de a păstra în format letric sau în format electronic, într-o formă admisă în procedurile judiciare, toate înregistrările obținute prin aplicarea acestor măsuri, cum ar fi copii ale documentelor de identificare, ale monitorizărilor și verificărilor efectuate, inclusiv, dacă sunt disponibile, ale informațiilor obținute prin mijloacele de identificare electronică, servicii de încredere relevante prevăzute în Regulamentul (UE) 910/2014 al Parlamentului European și al Consiliului din 23 Iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE sau orice alt proces de identificare sigur, la distanță sau electronic, reglementat, recunoscut, aprobat sau acceptat de către Autoritatea pentru Digitalizarea României necesare pentru respectarea cerințelor de cunoaștere privind clientela, pentru o perioadă de 5 ani de la data încetării relației de afaceri cu clientul ori de la data efectuării tranzacției ocazionale."

Ca atare, față de cele de mai sus, raportat la conținutul solicitării, având în vedere punctul de vedere al Băncii Naționale a României, anexat adresei petentei, ținând cont de prevederile legale mai sus menționate, în special cele ale art. 17 alin. 3 lit. a) din Regulamentul (UE) 2016/679, art. 8 și art. 50 din Legea nr. 93/2009 precum și art. 21 alin. (1) și 22 alin. (1) din Legea nr. 129/2019, Autoritatea națională de supraveghere a concluzionat că datele cu caracter personal ale clienților cu care instituțiile financiare nebanzare au negociat tranzacții, chiar dacă respectivele tranzacții nu s-au finalizat, sunt prelucrate (inclusiv stocate) de acești operatori în temeiul prevederilor art. 6 lit. (c) din Regulamentul (UE) 2016/679.



♦ **Dezvăluirea de date personale ale angajaților unei regi autonome către o primărie**

O regie autonomă a solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la solicitarea primită din partea unei primării de municipiu privind dezvăluirea datelor angajaților conținute în statul de personal al Regiei.

În acest context, față de cele de mai sus, raportat la conținutul adresei, Autoritatea națională de supraveghere a precizat că Ordonanța de Urgență a Guvernului nr. 109/2011 privind guvernarea corporativă a întreprinderilor publice definește, la art. 2 pct.3 lit.c), autoritatea publică tutelară ca fiind instituția care "coordonează exercitarea de către una sau mai multe întreprinderi publice prevăzute la pct. 2 lit. a) și/sau lit. b) a calității de acționar sau asociat la o societate controlată". În același timp, art. 58 conține dispoziții cu privire la conținutul Raportului anual emis de autoritatea publică tutelară, privitor la întreprinderile publice aflate în subordine, în coordonare, sub autoritate ori în portofoliu, printre informațiile conținute neregăsimdu-se și Statul de personal, astfel cum a fost solicitat de Primăria de municipiu în discuție, în calitate de acționar/asociat al Regiei.

În concluzie, având în vedere aspectele menționate mai sus și față de cele expuse în adresa transmisă, Autoritatea națională de supraveghere a precizat că datele angajaților conținute în statul de personal al Regiei, întreprindere publică sub autoritatea Consiliului Local, nu pot fi dezvăluite către primăria municipiului care a solicitat aceste date, în calitate de acționar/asociat al Regiei, decât în condițiile prevăzute de art. 6 din Regulamentul (UE) 2016/679, ținând cont totodată de respectarea principiilor de prelucrare, în special a principiului reducerii la minim a datelor.

♦ **Prevederile legale aplicabile în cazul utilizării unor drone pentru efectuarea de măsurători topografice**

O persoană fizică a solicitat un punct de vedere referitor la prevederile legale aplicabile în cazul utilizării unor echipamente de tip dronă pentru efectuarea de măsurători topografice.

În acest context s-a precizat că, în ceea ce privește informațiile ce pot fi considerate date cu caracter personal, potrivit art. 4 pct. 1 din Regulamentul (UE) 2016/679 „datele cu caracter personal” înseamnă „orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”)”.



Totodată, în ceea ce privește noțiunea de "operator" s-a precizat că, potrivit art. 4 pct. 7 din Regulamentul (UE) 2016/679, acesta este persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal.

În același timp, s-a subliniat faptul că prelucrările de date efectuate trebuie să fie precedate de o informare clară, concisă, într-un limbaj simplu, în conformitate cu art. 13 din Regulamentul (UE) 2016/679, care obligă operatorul să furnizeze persoanei vizate o serie de informații. În acest sens se poate efectua o informare publică pe site-ul operatorului.

În acest context, Autoritatea națională de supraveghere a subliniat faptul că situațiile expuse sunt aplicabile dispozițiile Regulamentului nr. 947/2019 privind normele și procedurile de operare a aeronavelor fără pilot la bord care, în Anexa I Partea B punctul V alin. (1) lit. a subpunctul (iv), prevede că:

"Operatorul UAS trebuie să întrunească toate condițiile enumerate în continuare:

(a) să stabilească proceduri și limitări adaptate tipului de operațiune avută în vedere și riscurilor implicate, inclusiv:

(iv) proceduri care să asigure că toate operațiunile respectă Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date. În special, operatorul UAS trebuie să efectueze o evaluare a impactului asupra protecției datelor la cererea autorității naționale pentru protecția datelor în conformitate cu articolul 35 din Regulamentul (UE) 2016/679;"

În același timp, Autoritatea națională de supraveghere a subliniat că sunt aplicabile dispozițiile Hotărârii Guvernului nr. 859/2021 pentru aprobarea procedurii de autorizare a zborurilor cu aeronave în spațiul aerian național, care în art. 15 prevede: "Orice activitate care implică prelucrarea datelor cu caracter personal, realizată în aplicarea prevederilor prezentei hotărâri, se efectuează cu respectarea prevederilor Regulamentului (UE) 2016/679."

♦ **Utilizarea de sisteme de supraveghere video de către unități de învățământ**

O societate a solicitat un punct de vedere referitor la utilizarea de sisteme de supraveghere video de către unități de învățământ.



Având în vedere conținutul solicitării, Autoritatea națională de supraveghere a subliniat următoarele aspecte cu caracter general:

Prelucrarea datelor cu caracter personal prin utilizarea unor sisteme de televiziune cu circuit închis cu posibilități de înregistrare și stocare a imaginilor și datelor se supune, în prezent, atât prevederilor Regulamentului (UE) 2016/679, cât și ale Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, modificată și completată.

În plus, în contextul celor de mai sus, Autoritatea națională de supraveghere a precizat că, prin raportare la prevederile art. 12 alin. (1) - (3) din Ordinul nr. 5241/2022 privind organizarea și desfășurarea evaluării naționale pentru absolvenții clasei a VIII-a, în anul școlar 2022-2023, **numai pe perioada desfășurării examenelor naționale există obligație legală pentru efectuarea supravegherii video în sălile de clasă.**

Cât privește utilizarea de camere de supraveghere video în sălile de curs în afara desfășurării examenelor mai sus amintite, precum și în alte spații pe care le administrează o unitate de învățământ, s-a precizat că aceasta se poate efectua numai cu îndeplinirea condițiilor prevăzute de art. 6 alin. (1) din Regulamentul (UE) 2016/679, cu condiția respectării principiilor de prelucrare și a drepturilor persoanelor vizate, în special cel al informații.

Autoritatea națională de supraveghere a subliniat faptul că prelucrările de date efectuate trebuie precedate de o informare clară, concisă, într-un limbaj simplu, în conformitate cu art. 13 din Regulamentul (UE) 2016/679, care obligă operatorul să furnizeze persoanei vizate o serie de informații. De asemenea, s-a precizat că, în spațiile monitorizate trebuie instalată o pictogramă adecvată, care să conțină o imagine reprezentativă, poziționată la o distanță rezonabilă de locul unde sunt amplasate echipamentele de supraveghere, astfel încât să poată fi văzută de orice persoană.

În acest context, referitor la prelucrarea datelor minorilor, Autoritatea națională de supraveghere a subliniat faptul că Regulamentul (UE) 2016/679 creează un nivel suplimentar de protecție în cazul în care sunt prelucrate datele cu caracter personal ale persoanelor fizice vulnerabile, în special ale copiilor. Considerentul 38 al Regulamentului (UE) 2016/679 prevede: „Copiii au nevoie de o protecție specifică a datelor lor cu caracter personal, întrucât pot fi mai puțin conștienți de riscurile, consecințele, garanțiile în cauză și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal”.



În plus, în contextul prelucrării datelor minorilor, s-a precizat că este necesară și respectarea dispozițiilor Legii nr. 272/2004 privind protecția și promovarea drepturilor copilului, urmând a fi avute în vedere prevederile art. 6, art. 27, art. 28, art. 29, art. 34, art. 37, art. 52 și art. 57 acest act normativ.

Prin urmare, raportat la reglementările din domeniul educației și la prevederile art. 5-7 din Regulamentul (UE) 2016/679, Autoritatea națională de supraveghere a precizat că datele (imagine/voce) nu pot fi prelucrate de un operator de date cu caracter personal (unitate de învățământ), decât cu consimțământul persoanelor vizate (angajați, elevi, respectiv reprezentanții legali ai acestora din urmă), ori în măsura în care există un temel legal expres pentru această prelucrare, cu respectarea principiilor de prelucrare a datelor și cu informarea persoanelor vizate.

În acest context, Autoritatea națională de supraveghere a recomandat și consultarea Ministerului Educației Naționale, raportat la competențele sale legale.

În ceea ce privește supravegherea video a spațiilor publice precum trotuare și parcuri, din imediata apropiere a unităților de învățământ Autoritatea națională de supraveghere a subliniat că, în măsura în care unitatea de învățământ stabilește și scopul prelucrării, aceasta are calitatea de operator de date cu caracter personal și, prin urmare, îi revin obligațiile din Regulamentul (UE) 2016/679, anterior menționate.

• **Aplicabilitatea Regulamentului (UE) 2016/679, raportat la conținutul**

certificatelor de concediu medical eliberate asiguratorilor

O persoană fizică, în calitate de cercetător, a solicitat Autorității naționale de supraveghere un punct de vedere privind aplicarea Regulamentului (UE) 2016/679 și a principiilor privind prelucrările de date în contextul relațiilor de muncă, raportat la conținutul certificatelor de concediu medical eliberate asiguratorilor din sistemul asigurărilor sociale de sănătate și din sistemul de asigurare pentru accidente de muncă și boli profesionale.

Situația se analizează raportat la dispozițiile art. 9 din Regulamentul (UE) 2016/679, cu informarea prealabilă a persoanelor vizate și cu respectarea principiilor stabilite de Regulamentul (UE) 2016/679 (în special al reducerii la minimum a datelor).

În contextul celor de mai sus, referitor la conținutul certificatului medical și la prelucrarea datelor cu caracter personal conținute de acest document de către angajator, Autoritatea națională de supraveghere a subliniat următoarele:



Ordonanța de Urgență a Guvernului nr. 158/2005 privind concediile și indemnizațiile de asigurări sociale de sănătate, cu modificările și completările ulterioare prevede, în art. 11 și art. 11¹ următoarele:

"Art. 11

(1) Asigurații beneficiază de concedii și de indemnizații, în baza certificatului medical eliberat de medicul curant, conform reglementărilor în vigoare.(...)

(3) Medicii prevăzuți la alin. (1) pot completa certificatele de concediu medical atât pe suport hârtie, cât și electronic și le pot transmite pe suport hârtie sau prin mijloace electronice de transmitere la distanță angajatorilor/persoanelor în drept, după caz.

(4) Certificatele de concediu medical, prevăzute la alin. (3), care sunt transmise prin mijloace electronice de transmitere la distanță de către medicii care le eliberează, sunt semnate de aceștia cu semnături electronice calificate."

Art. 11¹

Medicii prevăzuți la art. 11 au obligația de a completa certificatele de concediu medical cu respectarea Instrucțiunilor privind utilizarea și modul de completare a certificatelor de concediu medical, aprobate prin ordin comun al ministrului sănătății și al președintelui CNAS."

În același timp, Ordinul nr. 1192/2020 pentru aprobarea modelului unic al certificatului de concediu medical și a instrucțiunilor privind utilizarea și modul de completare a certificatelor de concediu medical pe baza cărora se acordă indemnizații asiguraților din sistemul asigurărilor sociale de sănătate și din sistemul de asigurare pentru accidente de muncă și boli profesionale, cu modificările și completările ulterioare, conține în Anexa nr. 1, Modelul unic de certificat medical și în Anexa 2 - Instrucțiuni din 1 iulie 2020 privind utilizarea și modul de completare a certificatelor de concediu medical.

În contextul aspectelor supuse atenției Autorității naționale de supraveghere și analizate prin raportare la prevederile legale anterior precizate, au fost efectuate demersuri la Ministerul Sănătății, cu propunerea de reanalizare a Ordinului nr. 1192/2020.

♦ **Dezvăluirea de date personale din registrele agricole în vederea realizării lucrărilor de cadastrare sistematică**

O autoritate publică locală (primărie) a solicitat opinia Autorității naționale de supraveghere cu privire la dezvăluirea datelor cu caracter personal din registrele agricole, în vederea realizării lucrărilor de cadastrare sistematică.



Referitor la modalitatea de prelucrare a datelor cu caracter personal, inclusiv sub aspectul colectării, stocării, divulgării prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, potrivit Regulamentului (UE) 2016/679, s-a precizat că aceasta se realizează cu consimțământul persoanei vizate sau în alte condiții legale în care nu se solicită consimțământul prevăzute de art. 6, art. 9 sau art. 10, în funcție de natura datelor și categoriilor de date colectate și prelucrate.

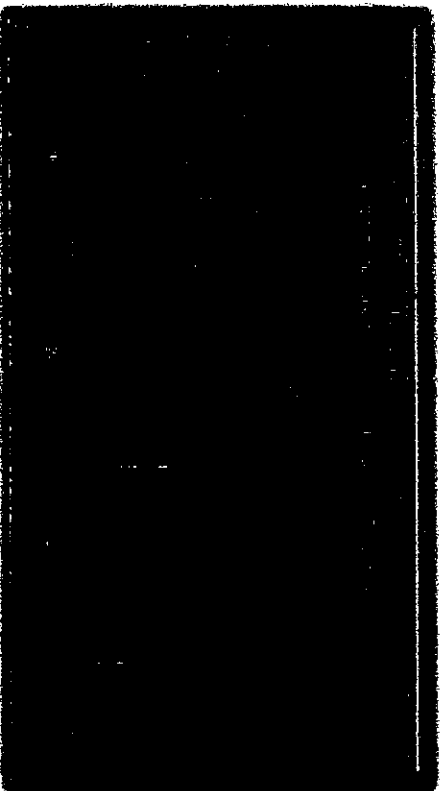
Autoritatea națională de supraveghere a mai arătat faptul că în cadrul prelucrării datelor este necesară respectarea principiilor stabilite de art. 5 din Regulamentul (UE) 2016/679, inclusiv principiul responsabilității, potrivit căruia operatorul este responsabil de respectarea acestor principii și poate demonstra această respectare.

În concluzie, s-a arătat că, având în vedere contractul de servicii încheiat între Agenția Națională de Cadastru și Publicitate Imobiliară și societatea care realizează lucrările de cadastrare, ce conține prevederi referitoare la prelucrarea datelor cu caracter personal), precum și prevederile Legii nr. 7/1996 a cadastrului și a publicității imobiliare, raportat la prevederile art. 6 alin. (1) lit. b), c) și e) din Regulamentul (UE) 2016/679, există temei legal pentru dezvăluirea datelor cu caracter personal în vederea furnizării serviciilor de înregistrare sistematică în Sistemul Integrat de Cadastru și Carte Funciară.

De asemenea, s-a precizat că entităților implicate le revine obligația de a lua toate măsurile necesare pentru respectarea drepturilor persoanelor vizate, precum și pentru asigurarea securității și confidențialității datelor, raportat la prevederile legale din domeniul de activitate.

■ **Puncte de vedere privind unele cauze aflate pe rolul Curtii de Justiție a Uniunii Europene**

În anul 2022 au fost transmise analize ale Autorității naționale de supraveghere către Ministerul Afacerilor Externe, în 30 cauze pendinte în fața Curții de Justiție a Uniunii Europene, în număr mai mare față de anii anteriori.



Cauzele analizate au avut ca obiect interpretarea anumitor articole din acte normative comunitare (Regulamentul (UE) 2016/679, Directiva 2016/680, Directiva 2002/58/CE, Regulamentul (UE) 2019/1157, Regulamentul (UE) 2018/858, TFUE, Carta UE precum și din alte acte comunitare ce conțin prevederi cu implicații în ceea ce privește prelucrarea datelor cu caracter personal), astfel:

- ▶ Cauza C-115/22 în cadrul căreia cererea a fost adresată de o instanță din Austria, referitoare la interpretarea dispozițiilor art. 9, 6 alin. (3), 5 alin. (1) lit. a) și c) și art. 10 din Regulamentul (UE) 2016/679, raportat la normele anti-doping.
- ▶ Cauza C-456/22 în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea dispozițiilor art. 82 alin. (1) din Regulamentul (UE) 2016/679.
- ▶ Cauza C-590/22 în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea dispozițiilor art. 82 alin. (1) din Regulamentul (UE) 2016/679.
- ▶ Cauza C-33/22 în cadrul căreia cererea a fost adresată de o instanță din Austria, referitoare la interpretarea art. 267 TFUE.

- ▶ Cauza C-60/22 în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea art. 5 alin. (2), art. 17 alin. (1) lit. d) și art. 18 alin. (1) lit. b) din Regulamentul (UE) 2016/679.
- ▶ Cauza C-61/22 în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea art. 3 alin. (5) din Regulamentul (UE) 2019/1157, raportat la art. 77 alin. (2) din TFUE, art. 7 și 8 din Carta UE și art. 35 alin. (10) din Regulamentul (UE) 2016/679.
- ▶ Cauza C-333/22 în cadrul căreia cererea a fost adresată de o instanță din Belgia, referitoare la interpretarea dispozițiilor 47 și 8 alin. (3) din Carta UE și art. 17 din Directiva 2016/680.
- ▶ Cauza C-461/22 în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea dispozițiilor art. 4 pct. 7 raportat la art. 15 din Regulamentul (UE) 2016/679.
- ▶ Cauza C-807/21 în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea dispozițiilor art. 83 alin. (4) – (6) din Regulamentul (UE) 2016/679.
- ▶ Cauza C-634/21 în cadrul căreia cererea a fost adresată de o instanță din Germania cu privire la interpretarea dispozițiilor art. 22 din Regulamentul (UE) 2016/679.
- ▶ Cauza C-178/22 în cadrul căreia cererea a fost adresată de o instanță din Italia, referitoare la interpretarea art. 15 alin. (1) din Directiva 2002/58/CE.
- ▶ Cauza C-182/22, în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea dispozițiilor art. art. 82 din Regulamentul (UE) 2016/679.
- ▶ Cauza C-118/22, în cadrul căreia cererea a fost adresată de o instanță din Bulgaria, referitoare la interpretarea dispozițiilor art. 5 coroborat cu art. 13 alin. (2) lit. b) din Directiva 2016/680.
- ▶ Cauza C-768/21, în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea dispozițiilor art. 57 alin. (1) lit. (a) și (f) și art. 58 alin. (2) lit. (a)-(f) coroborate cu art. 77 alin. (1) din Regulamentul (UE) 2016/679.
- ▶ Cauza C-306/21, în cadrul căreia cererea a fost adresată de o instanță din Bulgaria, referitoare la interpretarea dispozițiilor art. 2 alin. (2) și a art. 6 alin. (1) lit. e) din Regulamentul (UE) 2016/679, în legătură cu organizarea alegerilor din Bulgaria pentru



Adunera Națională și cu interzicerea înregistrării video cu ocazia deschiderii uanelor și a stabilirii rezultatelor alegerilor.

▶ Cauza C-683/21 în cadrul căreia cererea a fost adresată de o instanță din Lituania, cu privire la interpretarea dispozițiilor art. 4 pct. 7, prin raportare la art. 4 pct. 2, art. 26 alin. (1) și art. 83 alin. (1) din Regulamentul 2016/679.

▶ Cauza C-741/21 în cadrul căreia cererea a fost adresată de o instanță din Germania (Landgericht Saarbrücken), cu privire la interpretarea dispozițiilor art. 82, respectiv art. 83 din Regulamentul (UE) 2016/679.

▶ Cauzele conexate C-17/22 și C-18/22 (HTB Neunte Immobilien Portfolio geschlossene Investment UG & Co. KG), în cadrul cărora cererea a fost adresată de o instanță din Germania (Amtsgericht München), referitoare la interpretarea dispozițiilor art. 6 alin. (1) lit. b) și f) din Regulamentul (UE) 2016/679.

▶ Cauzele preliminare conexate C-26/22 și C-64/22 (SCHUFA Holding și alții), în cadrul căreia cererea a fost adresată de o instanță din Germania, raportat la întrebările adresate Curții referitoare la interpretarea art. 77 alin. (1), coroborat cu art. 78 alin. (1), art. 79, art. 17 alin. (1) lit. d) și art. 6 alin. (1) lit. f) și art. 40 din Regulamentul (UE) 2016/679.

▶ Cauza C-162/22 în cadrul căreia cererea a fost adresată de o instanță din Lituania (Lietuvos Respublikos generalinė prokuratūra - Lituania), privind interpretarea art. 15 alin. (1), coroborat cu art. 7, 8, 11 și 52 din Carta Drepturilor Fundamentale a Uniunii Europene.

▶ Cauza C-231/22 în cadrul căreia cererea a fost adresată de o instanță din Belgia, cu privire la interpretarea dispozițiilor art. 4 pct. 7, respectiv art. 5 alin. (2) din Regulamentul (UE) 2016/679.

▶ Cauza C-241/22 în cadrul căreia cererea a fost adresată de o instanță din Țările de Jos, raportat la întrebările adresate Curții referitoare la domeniul de aplicare al Directivei 2002/58 și interpretarea noțiunilor „infracțiuni grave” și „infracționalitate gravă”, precum și posibilitatea de a acorda autorităților publice accesul la date de trafic și localizare (altele decât datele cu rol exclusiv de identificare), respectiv interpretarea articolelor 1, 2, 3, 5, 6, 9 și 15 alineatul (1) al Directivei 2002/58.

▶ Cauza C-307/22, în cadrul căreia cererea a fost adresată de o instanță din Germania cu privire la interpretarea art. 15 alin. (3) din Regulamentul (UE) 2016/679 coroborat cu art. 12 alin. (5) din Regulamentul (UE) 2016/679, raportat și la dispozițiile art. 23 alin. (1) lit. i) din Regulamentul (UE) 2016/679.



▶ C-604/22 în cadrul căreia cererea a fost adresată de o instanță din Belgia, referitoare la interpretarea dispozițiilor art. 4 pct. 1 din Regulamentul (UE) 2016/679 și art. 4 pct. 7 din Regulamentul (UE) 2016/679 prin raportare art. 24 alin. (1) din Regulamentul (UE) 2016/679 și art. 7 și art. 8 din Carta Drepturilor Fundamentale a Uniunii Europene.

▶ Cauza C-693/22 raportat la întrebările formulate de o instanță din Polonia privind interpretarea dispozițiilor art. 5 alin. (1) lit. a) coroborate cu art. 6 alin. (1) lit. a), c) și e) și art. 6 alin. (3) din Regulamentul (UE) 2016/679.

▶ Cauza C-672/22 în cadrul căreia cererea a fost adresată de o instanță din Germania, întrebările preliminare fiind legate de interpretarea dispozițiilor art. 15 alin. (3) prima teză din Regulamentul (UE) 2016/679 privind furnizarea unei copii a datelor cu caracter personal care fac obiectul prelucrării.

▶ Cauza C-319/22 în cadrul căreia cererea a fost adresată de o instanță din Germania (Landgericht Köln), referitoare la interpretarea art. 61 din Regulamentul (UE) 2018/858 al Parlamentului European și al Consiliului privind omologarea și supravegherea pieței autovehiculelor și remorcilor acestora, precum și ale sistemelor, componentelor și unităților tehnice separate destinate vehiculelor respective, de modificare a Regulamentelor (CE) nr. 715/2007 și (CE) nr. 595/2009 și de abrogare a Directivei 2007/46/CE.

▶ Cauza C-280/22 în cadrul căreia cererea a fost adresată de o instanță din Belgia, întrebarea preliminară fiind legată de interpretarea art. 3 alin. (5) și (6) și art. 14 din Regulamentul (UE) 2019/1157 al Parlamentului European și al Consiliului privind consolidarea securității cărților de identitate ale cetățenilor Uniunii și a documentelor de ședere eliberate cetățenilor Uniunii și membrilor de familie ai acestora care își exercită dreptul la liberă circulație.

▶ Cauza C-621/22, în cadrul căreia cererea a fost adresată de o instanță din Țările de Jos (Amsterdam), raportat la întrebările adresate Curții referitoare la dispozițiile art. 6 alin. (1) lit. f) din Regulamentul (UE) 2016/679.

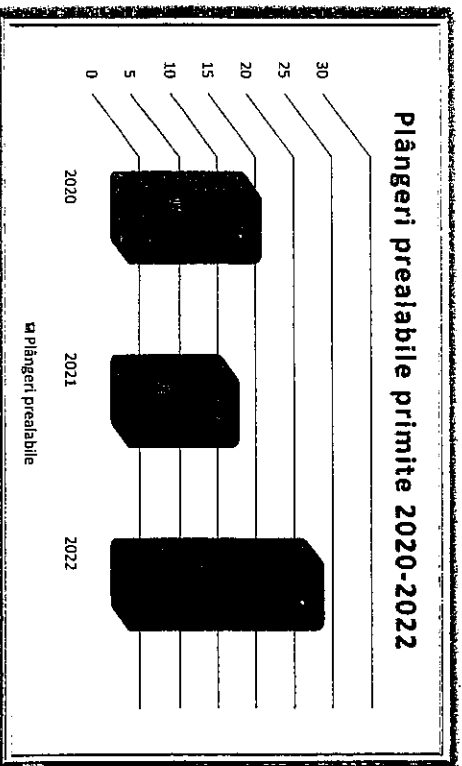
▶ Cauza C-659/22 în cadrul căreia cererea a fost adresată de o instanță din Republica Cehă, raportat la întrebarea adresată Curții referitoare la interpretarea dispozițiilor art. 4 punctul 2 din Regulamentul (UE) 2016/679, prin raportare la aplicarea domeniului material stabilit de art. 2 alin. (1) din același regulament.

■ **Activitatea de analiză și soluționare a plângerilor prelabile**

Potrivit art. 21 alin. (6) din Legea nr. 102/2005, republicată, în măsura în care persoana vizată este nemulțumită de răspunsul primit ca urmare a depunerii plângeri sale la Autoritatea națională de supraveghere, aceasta se poate adresa secției de contencios administrativ a tribunalului competent, după parcurgerea procedurii prelabile prevăzute de Legea contenciosului administrativ nr. 554/2004, cu modificările și completările ulterioare.

Astfel, pe parcursul **anului 2022** au fost depuse la Autoritatea națională de supraveghere un număr de **26 plângeri prelabile**.

Dintre plângerile prelabile formulate în condițiile legii, urmare a reanalizării susținerilor și dovezilor transmise de către petenți, **au fost admise 6**, raportat la aspectele semnalate de către persoanele vizate în situațiile respective.



Secțiunea a 3 – a

Activitatea de reprezentare în fața instanțelor de judecată

În anul **2022**, **Autoritatea națională de supraveghere a gestionat un număr de 108 dosare aflate pe rolul instanțelor de judecată în diferite stadii procesuale.**

Dintre acestea, **pe parcursul anului 2022** au fost înregistrate pe rolul instanțelor de judecată un număr de **40 de cereri noi de chemare în judecată** întemelte pe Regulamentul (UE) 2016/679 sau pe Legea nr. 554/2004 a contenciosului administrativ.

Menționăm că, **din cele 40 de cereri de chemare în judecată, 22 cereri de chemare în judecată au avut ca obiect contestarea proceselor – verbale de constatare/sancționare încheiate de Autoritatea națională de supraveghere.**

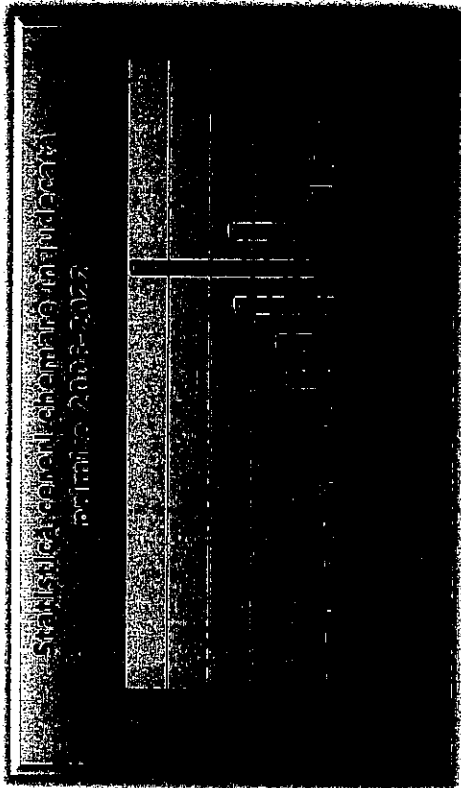
În ceea ce privește **contestarea sancțiunilor cu amendă dispuse de către Autoritatea națională de supraveghere după punerea în aplicare a Regulamentului (UE) 2016/679**, este de remarcat faptul că, **din totalul de 162 amenzi aplicate operatorilor în perioada 2019 -2022**, în baza Regulamentului (UE) 2016/679, **au fost contestate în instanțe doar 42 de amenzi.**

Din cele **42 de dosare în instanțe ce au avut ca obiect contestarea amenzii**, au fost până în prezent **definitivate 20 dosare**, iar în **15 dintre aceste cauze au fost pronunțate soluții definitive în favoarea Autorității naționale de supraveghere.**

Astfel, **instanțele de judecată au confirmat integral amenzile aplicate de instituția noastră operatorilor în 10 litigii.**

În plus, au fost soluționate în favoarea Autorității naționale de supraveghere, prin **menținerea proceselor-verbale de constatare/sancționare în sensul reținerii caracterului contravențional al faptelor**, cu diminuarea cuantumului amenzii sau înlocuirea acesteia cu avertisment, în **alte 5 litigii.**

Pe de altă parte, menționăm că au fost admise plângerile contravenționale formulate de 5 operatori, raportat la perioada 2019-2022.



În anul 2022, au fost finalizate definitiv mai multe acțiuni în mod favorabil pentru instituția noastră, dintre care prezentăm mai jos câteva cazuri relevante:

• **Hotărâre definitivă pronunțată într-un litigiu privind încălcarea art. 6 și art. 21 din Regulamentul (UE) 2016/679**

Autoritatea națională de supraveghere a efectuat o investigație în anul 2020, ca urmare a unei plângeri a unui petent prin care acesta sesiza încălcarea dreptului său de opoziție de un operator din domeniul vânzărilor online.

În cadrul acestei investigații s-a constatat că la sfârșitul anului 2019 acest operator a transmis unei persoane fizice un mesaj comercial, deși la începutul anului 2019 operatorul îi confirmase acesteia dezabonarea de la comunicările comerciale.

Prin urmare, operatorul din domeniul vânzărilor on-line a fost sancționat contravențional cu amendă în cuantum de 14.420,4 lei (echivalentul a 3.000 EURO).

În același timp, operatorului i s-au aplicat și următoarele măsuri corective:

- să implementeze solicitarea petentului de a-i fi dezactivată din baza de date setarea privind transmiterea pe adresa sa de e-mail a mesajelor comerciale, în termen de 3 zile lucrătoare de la comunicarea procesului-verbal de contravenție (art. 58 alin. (2) lit. c);

- să ia măsuri astfel încât să fie respectate, în toate cazurile, prevederile art. 21 Regulamentului (UE) 2016/679.

În acest context, menționăm că art. 21 alin. (3) din Regulamentul (UE) 2016/679 prevede că "în cazul în care persoana vizată se opune prelucrării în scopul marketingului direct, datele cu caracter personal nu mai sunt prelucrate în acest scop."

Operatorul a contestat în instanță procesul-verbal de constatare/sancționare încheiat de Autoritatea națională de supraveghere.

Analizând probatoriul administrat în cauză, Tribunalul București a admis în parte cererea de chemare în judecată formulată de operator și a dispus înlocuirea sancțiunii amenzii cu aceea a avertismentului.

Cu privire la temeinicia procesului-verbal de contravenție, instanța a apreciat că *"procesul verbal a fost legal și temeinic întocmit"*.

Autoritatea națională de supraveghere și operatorul din domeniul vânzărilor on-line au formulat apel.

Curtea de Apel București a respins apelul formulat de operatorul din domeniul vânzărilor on-line, ca nefondat.

Totodată, Curtea de Apel București a admis apelul formulat de Autoritatea națională de supraveghere și a schimbat în parte sentința apelată, în sensul că a respins în integralitate plângerea contravențională ca neintemeiată.

Cu privire la cuantumul amenzii, Curtea de Apel București a apreciat că: *"În cauză, sancțiunea aplicată de autoritate corespunde pe deplin acestor cerințe de proporționalitate în condițiile în care, astfel cum s-a reținut deja, fapta a fost săvârșită în condițiile în care persoana care a formulat sesizarea solicitase în mod expres ca apelantul-reclamant să nu-i mai transmită mesaje cu caracter comercial."*

Totodată, din cuprinsul cererii de chemare în judecată și a cererii de apel nu reiese că apelantul-reclamant a înțeles faptul că a realizat o prelucrare nelegală, argumentele sale fiind centrate pe faptul că a acționat pe deplin în conformitate cu dispozițiile legale, prin încercarea de a masca sub aparența unui mesaj tranzacțional a unui mesaj de marketing direct. De asemenea, Curtea constată că apelantul-reclamant a mai fost sancționat pentru încălcări ale prevederilor legale referitoare la prelucrarea datelor cu caracter personal (...).

Pe de altă parte, cuantumul amenzii stabilite de apelantul-pârât prin procesul verbal de contravenție (echivalentul a 3000 euro) este orientat spre minimul special stabilit de lege

și are o valoare cu mult mai mică decât sancțiunile aplicate altor operatori economici pentru fapte similare.”

Pe cale de consecință, Curtea de Apel București a confirmat corectitudinea procesului-verbal încheiat și a amenzi aplicate de instituția noastră.

Hotărârea judecătorească, favorabilă Autorității naționale de supraveghere, a rămas definitivă.

• Hotărâre definitivă pronunțată într-un litigiu privind încălcarea art. 5 alin. (1) lit. f) și art. 32 alin. (1) din Regulamentul (UE) 2016/679

Autoritatea națională de supraveghere a efectuat o investigație, în anul 2020, în urma primirii unor sesizări cu privire la încălcarea confidențialității și securității datelor personale.

În cadrul acestei investigații s-a constatat că a avut loc dezvăluirea în spațiul public (on-line) a declarației solicitate de operatorul din domeniul-finanțiar bancar (banca) unui client al său, cu privire la modul în care intenționa să utilizeze o anumită sumă de bani pe care acesta dorea să o ridice din contul său. Această declarație a fost distribuită între câțiva angajați ai băncii pe adresele de e-mail de serviciu. Unul dintre angajații a listat e-mailul ce conținea declarația clientului, precum și e-mailul ce conținea conversația internă între angajații operatorului. Un alt angajat a fotografiat cu telefonul mobil înscrisul listat și l-a distribuit prin intermediul aplicației WhatsApp. Ulterior, înscrisul listat a fost postat și distribuit atât pe rețeaua de socializare Facebook, cât și pe un site.

Această situație a condus la dezvăluirea și accesul neautorizat la anumite date cu caracter personal (nume și prenume, adrese de e-mail, date comportamentale, preferințe personale, valoare tranzacție financiară, adresa locului de muncă, funcție și locul muncii, număr de telefon de serviciu) a 4 persoane fizice vizate (un client și 3 angajați proprii), deși potrivit art. 5 lit. f) din Regulamentul (UE) 2016/679, operatorul avea obligația de a respecta principiul integrității și confidențialității datelor personale.

Astfel, s-a reținut că operatorul nu a luat măsuri suficiente pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea sa (salariații proprii) și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului.

Dezvăluirea produsă în spațiul public dovedește și ineficiența instruirii interne a angajaților operatorului privind respectarea normelor de protecția datelor cu caracter personal ale persoanelor vizate, deși instruirea angajaților este parte intrinsecă a măsurilor

tehnice și organizatorice pe care operatorul era obligat să le adopte în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, încălcându-se astfel prevederile art. 32 din Regulamentul (UE) 2016/679.

În acest context, s-a avut în vedere și că dezvăluirea datelor cu caracter personal în spațiul public (pe internet) a generat o serie de prejudicii de natură morală, precum și alte dezavantaje semnificative de natură economică sau socială pentru persoana fizică afectată de producerea incidentului de securitate (client al băncii).

Prin urmare, operatorul a fost sancționat contravențional cu amendă în cuantum de 487.380 lei (echivalentul a 100.000 EURO).

Procesul-verbal de constatare/sancționare a fost contestat de instituția financiar-bancară sancționată.

Instanța de fond – Tribunalul Cluj, în mod corect a reținut că: *”Înscrisurile prezentate de reclamantă, în dovedirea implementării măsurilor tehnice și organizatorice adecvate, nu sunt de natură să probeze asigurarea unui nivel de securitate corespunzător privind capacitatea de a asigura confidențialitatea și testarea, evaluarea și aprecierea periodică ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.”*

În ce privește consecințele încălcării, Tribunalul Cluj a reținut că *”acestora au fost corect calificate de către pătărită ca fiind grave prin raportare la cantitatea datelor cu caracter personal diseminate de angajații Băncii, natura sensibilă a acestora, modalitatea de diseminare (prin internet), (...) numărul extrem de mare al persoanelor care au dobândit acces la datele clientului Băncii pentru o perioadă de timp imposibil de determinat, urmare a transmiterii informațiilor prin mijloacele cele mai diverse, toate aceste aspecte fiind în măsură să confere o imagine corectă cu privire la amploarea și gravitatea consecințelor incidentului de securitate.*

Reclamanta a recunoscut, de altfel, raportat la modalitatea de transmitere a datelor cu caracter personal, că măsurile întreprinse pentru limitarea consecințelor breșei de securitate nu au fost ”fzabile”, amploarea diseminării acestora în spațiul public fiind în mod evident scăpată de sub control.”

În final, instanța de fond a concluzionat în mod corect faptul că:

«amenda în cuantum de 100.000 euro este legală, eficace, proporțională și disuasivă” și a fost stabilită cu luarea în considerare a naturii, gravității și consecințelor încălcării, precum și



tuturor celorlalte criterii prevăzute de Regulament, criteriile care au fost analizate de părâtă în mod coerent și obiectiv.»

Hotărârea instanței de fond, favorabilă Autorității naționale de supraveghere, a rămas definitivă prin respingerea apelului formulat de instituția financiar-bancară sancționată.

- **Hotărâre definitivă pronunțată într-un litigiu privind încălcarea prevederilor art. 25 alin. (1) și art. 32 din Regulamentul (UE) 2016/679**

Autoritatea națională de supraveghere a fost notificată în anul 2020 cu privire la producerea unei încălcări a securității datelor cu caracter personal la nivelul operatorului național din domeniul serviciilor poștale, conform prevederilor art. 33 din Regulamentul (UE) 2016/679.

În urma investigației s-a reținut că încălcarea securității și confidențialității datelor cu caracter personal a constat în faptul că operatorul nu a implementat măsuri tehnice și organizatorice adecvate (de exemplu, pseudonimizarea), atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, astfel încât să se pună în aplicare, în mod eficient, principiile de protecție a datelor și să se integreze în acestea garanțiile necesare prelucrării, astfel încât să fie duse la îndeplinire cerințele Regulamentului (UE) 2016/679 și să se protejeze drepturile persoanelor vizate.

Operatorul nu a luat măsurile tehnice și organizatorice adecvate care să prevină accesul neautorizat la datele cu caracter personal (adrese de e-mail și numere de telefon) pe adresa proprie de internet, ceea ce a dus la compromiterea confidențialității datelor personale a 81 de persoane vizate.

Prin urmare, operatorul a fost sancționat contravențional cu o amendă în cuantum de 9.686,60 lei (echivalentul a 2.000 euro), astfel:

- pentru încălcarea prevederilor art. 25 alin. (1) și art. 32 din Regulamentul (UE) 2016/679, în temeiul art. 58 alin. (2) lit. i) din Regulamentul (UE) 2016/679, coroborat cu art. 83 din Regulamentul (UE) 2016/679, raportate la art. 14 alin. (11) și art. 15 alin. (1) și alin. (6) din Legea nr. 102/2005, republicată, precum și la art. 12 din Legea nr. 190/2018 coroborat cu art. 8 din OG nr. 2/2001.

Procesul-verbal de constatare/sancționare a fost contestat de operatorul național din



domeniul serviciilor poștale sancționat.

Instanța de fond – Tribunalul București, în ceea ce privește modul de întocmire a procesului-verbal, în mod corect a reținut că *"procesul verbal contestat îmbracă toate condițiile de formă și de fond, nefiind regăsite, nici din oficiu, cauze de nulitate."*

Mai mult, cu privire la fondul și temeinicia actului sancționator, instanța de fond a reținut că *"reclamanta nu aduce critici esențiale, ci doar din perspectiva nelegalității."*

Totodată, instanța de fond a reținut *"Constatămăle păratei, ce au în vedere nerespectarea prev. art. 25 alin. (1) din Regulamentul (UE) 2016/679 se reflectă, de cu seamă în faptul că persoane fizice în această aplicație, au generat în mod aleatoriu alte coduri plecând de la cel alocat, aspect recunoscut de reclamantă în cele declarate în formularul de notificare al breșei."*

Reclamanta a mai arătat că au existat unele măsuri tehnice și organizatorice la nivelul operatorului anterior producerii incidentului de securitate cât și la momentul producerii acestuia, ori, o atare recunoaștere nu poate fi ulterior retrasă, decât în condițiile unui probatoriu consistent."

În ceea ce privește solicitarea de înlocuire a sancțiunii amenzii contravenționale cu măsura avertismentului, Tribunalul a reținut că, *întrucât "limita maxima ar fi putut ajunge la 10 000 000 EUR, sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală corespunzătoare exercitiului financiar anterior, potrivit dispozițiilor art. 83 alin. (4) din Regulamentul (UE) 2016/679 se constată că sancțiunea dispusă a fost orientată către minim, respectiv, sub jumătatea sancțiunii maxime ce se putea aplica, în condițiile în care, reclamanta nu a adus minim de dovezi care sa ateste gradul de pericol social redus al faptei, respectiv o disproporție vădită între faptă și sancțiunea aplicată."*

Prin urmare, Tribunalul a arătat că *"aplicarea sancțiunii amenzii contravenționale în cuantumul dispus (...) este proporțională cu gravitatea faptei săvârșite, nefiind identificate cauze care să-i înlăture răspunderea contravențională"*.

Hotărârea instanței de fond, favorabilă Autorității naționale de supraveghere, a rămas definitivă.

• Hotărâre definitivă pronunțată într-un litigiu privind încălcarea securității prelucrării

Autoritatea națională de supraveghere a fost notificată în anul 2019 cu privire la producerea unei încălcări a securității datelor cu caracter personal la nivelul unei instituții financiar-bancare, conform prevederilor art. 33 din Regulamentul (UE) 2016/679.

Conform notificării transmise a reieșit faptul că două angajate ale operatorului instituție financiar-bancară, utilizând datele din documentele de identitate ale unor persoane fizice, transmise de către angajați ai unei alte societăți, instituție financiar bancară, prin intermediul aplicației mobile WhatsApp, au efectuat interogări în sistemul Biroului de Credit SA, pentru a obține datele necesare în vederea determinării eligibilității la creditare a respectivelor persoane fizice vizate, print-o simulare de prescoring (1194 simulări de prescoring, cu privire la 1177 persoane fizice). De asemenea, pentru 124 de persoane fizice vizate s-a efectuat și consultarea bazei de date a Agenției Naționale de Administrare Fiscală.

Simulările de prescoring menționate mai sus au fost efectuate prin intermediul aplicației informatice utilizate de instituția financiar-bancară (bancă) în activitatea de creditare, cu încălcarea procedurilor interne. În urma simulărilor de prescoring menționate, decizia negativă de creditare a fost comunicată de angajatele băncii către angajații instituției financiare nebancale.

În acest context, Autoritatea națională de supraveghere a efectuat investigații la cele două entități.

În urma investigației derulate la operatorul instituție financiar-bancară s-a încheiat un proces-verbal de constatare/sancționare prin care a fost aplicată sancțiunea cu amendă în cuantum total de 712.680 lei (echivalentul a 150.000 euro) pentru:

- încălcarea art. 32 alin. (4) coroborat cu art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679, în temeiul art. 58 alin. (2) lit. 1) din Regulamentul (UE) 2016/679, raportat la art. 14 alin. (1) și art. 15 alin. (1) și alin. (6) din Legea nr. 102/2005, republicată, precum și la art. 12 din Legea nr. 190/2018 coroborat cu art. 8 din OG nr. 2/2001.

Procesul-verbal de constatare/sancționare a fost contestat de instituția financiar-bancară sancționată, iar instanța de fond – Tribunalul București, cu privire la Procesul-verbal de contravenție contestat, a reținut că acesta *”cuprinde toate mențiunile prevăzute de art. 17 din OG nr. 2/2001. De asemenea, fapta, săvârșită este descrisă, suficient, fiind redată conținutul, acestea.”*

Totodată, cu privire la fapta pentru care a fost sancționată instituția financiar-bancară, respectiv încălcarea prevederilor art. 32 alin.(4) coroborat cu art.32 alin.(1) și (2) din Regulamentul (UE) 2016/679, instanța de fond a reținut în mod corect circumstanțele săvârșirii acesteia.

Tribunalul București a respins apărările instituției financiar-bancare, arătând că *“(…) reclamația nu poate invoca în apărarea sa faptul că a luat toate măsurile pentru a preveni săvârșirea unor astfel de fapte, că incidentul a fost datorită eroii și relei credințe a unor angajați (reclamanța fiind ținută să răspundă pentru conduita angajaților săi) sau că pârâta nu a arătat ce măsuri trebuia să ia reclamația.”*

De asemenea, instanța de fond a respins apărările reclamantei, raportat și la Procedura de efectuare a investigațiilor, aprobată prin Decizia nr. 161/2018 a președintelui Autorității naționale de supraveghere, arătând că *”sunt neîntemeiate criticile reclamantei.”*

Cu toate acestea, instanța de fond a redus amenda aplicată.

Pentru a hotărî astfel, instanța a arătat că *”pe lângă limitele legale ale sancțiunii, trebuie avut în vedere faptul că reclamația a avut o conținută sinceră, incidentul în securitatea datelor fiind descoperit în urma sesizării acesteia, precum și că prin acțiunile reclamantei au fost înălturate consecințele incidentului de securitate prin ștergerea din sistemele informatice proprii, a evaluărilor preliminare ale eligibilității, efectuate neautorizat.”*

Hotărârea instanței de fond, parțial favorabilă Autorității naționale de supraveghere, a rămas definitivă.

• **Hotărâre definitivă pronunțată într-un litigiu privind încălcarea prevederilor art. 58 alin. (1) lit. a) și lit. e) din Regulamentul (UE) 2016/679**

Autoritatea națională de supraveghere a efectuat, în anul 2019, o investigație ca urmare a unor petiții prin care s-a sesizat faptul că operatorul prelucrează date cu caracter personal prin transmiterea de mesaje comerciale nesolicitate de tip SMS pe numărul personal de telefon al petentului, fără consimțământul său.

Operatorul nu a furnizat informațiile solicitate de Autoritatea națională de supraveghere în cadrul investigației și astfel s-a încheiat un proces-verbal de constatare/sancționare prin care s-a dispus sancționarea acestuia cu amendă în cuantum de 9.890 lei (echivalentul a 2.000 euro) pentru încălcarea prevederilor art. 58 alin. (1) din Regulamentul (UE) 2016/679.



Operatorul a contestat în instanță procesul – verbal de constatare/sancționare încheiat de Autoritatea națională de supraveghere.

Tribunalul Dolj a respins ca neîntemeiată plângerea formulată de operator.

Astfel, instanța de fond a reținut că „petența nu a comunicat informațiile solicitate de intimată, cu toate că acestea i-au fost adresate trei notificări în acest sens, motiv pentru care instanța consideră că în mod legal a fost constatată de către intimată contravenția prevăzută de art. 58 din Regulamentul (UE) 2016/679.”

De asemenea, „cu privire la intervenirea prescripției aplicării sancțiunii amenziilor contravenționale, instanța o va respinge ca neîntemeiată având în vedere faptul că potrivit art. 15 din Legea nr. 190/2018 sancțiunile contravenționale principale pe care le aplică Autoritatea națională de supraveghere, potrivit art. 58 alin. (2) lit. b) și l) din Regulamentul (UE) 2016/679, sunt avertismentul și amenda. Aplicarea amenziilor se face în condițiile art. 85 din Regulamentul (UE) 2016/679.

(4) Sancțiunile prevăzute la alin. (1) pot fi aplicate în termen de 3 ani de la data săvârșirii faptei. În cazul încălcărilor care durează în timp sau al celor constând în săvârșirea, în baza aceleiași rezoluții, la intervale diferite de timp, a mai multor acțiuni sau inacțiuni, care prezintă, fiecare în parte, conținutul aceleiași contravenții, prescripția începe să curgă de la data constatării sau de la data încetării ultimului act ori fapt săvârșit, dacă acest moment intervine anterior constatării.”

Referitor la individualizarea sancțiunii aplicate, „instanța constată că sancțiunea amenziilor în cuantum de 9890 lei, echivalentul a 2.000 euro, este proporțională cu gradul de pericol social al faptei săvârșite privind protecția datelor personale și cu dispozițiile art. 85 alin. (5) lit. e) din Regulamentul (UE) 2016/679.”

În ceea ce privește temeinicia procesului-verbal de contravenție, instanța a reținut că aceste este legal și temeinic întocmit.

Hotărârea instanței de fond, favorabilă Autorității naționale de supraveghere, a rămas definitivă.

• **Hotărâre definitivă pronunțată într-un litigiu privind încălcarea dispozițiilor art. 12 alin. (3), art. 15 alin. (1), art. 28 alin. (1) și 32, art. 33 din Regulamentul (UE) 2016/679**



Autoritatea națională de supraveghere a efectuat o investigație, în anul 2021, la un centru medical, ca urmare a unei plângeri prin care s-a reclamat faptul că operatorul a transmis o informare acestuia în legătură cu pierderea probelor sale biologice și a unei sume de bani trimise prin intermediul unei firme de curierat, coletul ajungând deteriorat la destinatar.

Astfel, la solicitarea unui pacient al centrului de a i se comunica ce date personale i-au fost expuse cu această ocazie și dacă Autoritatea națională de supraveghere a fost notificată în legătură cu acest incident, în răspunsul trimis, operatorul a indicat persoanei fizice datele de contact ale avocatului societății și o adresă de e-mail de la firma de curierat către care să își exprime “doleanțele”.

În cursul investigației demarate Autoritatea națională de supraveghere a constatat că centrul medical nu a adoptat suficiente măsuri de securitate, conform art. 28 alin. (1) și 32 din Regulamentul (UE) 2016/679, adaptate la caracterul datelor personale care au fost supuse prelucrării, fapt care a condus la producerea unui incident de încălcare a securității datelor cu caracter personal. În acest context, s-a constatat că nu au fost respectate prevederile art. 28 alin. (1) și art. 32 din Regulamentul (UE) 2016/679.

De asemenea, Autoritatea națională de supraveghere a constatat că operatorul nu a notificat incidentul de securitate produs, încălcând astfel prevederile art. 33 din Regulamentul (UE) 2016/679.

Cu aceeași ocazie, Autoritatea națională de supraveghere a reținut că operatorul nu a prezentat dovezi din care să rezulte că a comunicat un răspuns la adresa poștală a persoanei vizate (care a solicitat în mod expres aceasta) cu privire la categoriile de date personale ce i-au fost expuse cu ocazia incidentului produs. Prin urmare, s-a constatat că nu au fost respectate prevederile art. 12 alin. (3) și 15 alin. (1) din Regulamentul (UE) 2016/679.

Ca atare, operatorul a fost sancționat cu două amenzi în cuantum total de 14.754,9 lei (echivalentul a 3000 euro) și un avertisment.

De asemenea, operatorului i-au fost aplicate și următoarele măsuri corective:

- de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de prelucrare a datelor personale, prin punerea în aplicare a unor măsuri de securitate tehnice și organizatorice adecvate specificului prelucrării și riscurilor identificate, pe întreg ciclul de prelucrare a datelor, inclusiv sub aspectul alegerii unor persoane împuternicite care să prezinte garanții suficiente pentru punerea în aplicare a unor

măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în regulament și să asigure protecția drepturilor persoanelor vizate;

- de a răspunde la cererea persoanei vizate, privind categoriile de date personale vizate de producerea incidentului de securitate, urmând a-i comunica răspunsul la adresa poștală indicată în cerere.

Operatorul a contestat în instanță procesul-verbal de constatare/sanționare încheiat de Autoritatea națională de supraveghere.

Analizând probele cauzei, Tribunalul Mureș a respins acțiunea în contencios administrativ formulată de operator ca neîntemeiată.

În susținerea sale, instanța de fond a constatat faptul că "amenda în cuantumul aplicat este legală, eficace, proporțională și disuasivă și a fost stabilită cu luarea în considerare a naturii, gravității și consecințelor încălcării, precum și tuturor celorlalte criterii prevăzute de Regulament, criteriile care au fost analizate de pârâtă corect".

Tribunalul Mureș a subliniat că "Regulamentul a introdus un nivel mult mai ridicat de responsabilizare a operatorului de date în comparație cu Directiva 95/46/CE privind protecția datelor, iar articolele 25 și 32 din Regulament prevăd că operatorii au în vedere stadiul actual al tehnologiei, costurile implementării și natura, domeniul de aplicare, contextul, scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea.

Instanța a constatat: „Cu privire la temeinicia sancționării reclamantei (...) pârâta a făcut dovada că sunt întrunite elementele constitutive ale contravențiilor reținute. Totodată, reclamanta nu a probat existența unei alte stări de fapt, decât cea consemnată în procesul-verbal de constatare contestat.”

Curtea de Apel Târgu-Mureș a respins apelul formulat de operator.

Prin hotărârea dată, instanța de apel a reținut în legătură cu operatorul că "susținerea referitoare la lipsa sa de răspundere nu pot fi primite, dispozițiile cuprinse în contractele încheiate cu alte părți nefiind opozabile persoanelor care s-au adresat exclusiv (...), încredințându-i acesteia probele biologice."

În același sens, instanța a arătat că "în calitatea sa de operator de date cu caracter personal, (...) trebuia împreună cu persoana împuternicită să pună în aplicare măsuri tehnice și

organizatorice adecvate pentru ca drepturile și libertățile persoanelor fizice să nu fie puse în pericol, cu atât mai mult cu cât transportul cuprindea date sensibile, respectiv să se asigure că persoana împuternicită oferă garanții suficiente pentru punerea în aplicare a măsurilor tehnice și organizatorice."

De asemenea, instanța de apel a constatat că operatorul "nu face nicio referire la circumstanțele prezentate de persoana vizată de încălcarea securității datelor cu caracter personal. (...) Aceste circumstanțe sunt deosebit de grave întrucât sunt legate de starea de sănătate a persoanei în cauză, existând în mod evident pericolul ca aceasta să fie detentoră prin simpla trecere a timpului."

Hotărârea instanței de fond, favorabilă Autorității naționale de supraveghere, a rămas definitivă.

• **Hotărâre definitivă pronunțată într-un litigiu referitor la anularea unei decizii de măsuri a Autorității naționale de supraveghere.**

Autoritatea națională de supraveghere a efectuat o investigație, în anul 2020, ca urmare a unei sesizări referitoare la încălcarea legislației privind protecția datelor de către o Unitate Administrativă Teritorială, pentru o Direcție Generală de Poliție Locală.

Prin sesizare se semnală faptul că polițiștilor locali din cadrul Direcției Generale de Poliție Locală a Unității Administrative Teritoriale le-a fost stabilită obligația de a purta asupra lor, în timpul programului de lucru, camere de înregistrare audio – video de tip "Body-Worn Camera" (care au încorporată și funcția GPS), sens în care angajații instituției sunt monitorizați permanent.

În urma acestei investigații s-a constatat că operatorul – UAT pentru Direcția Generală de Poliție Locală a încălcat prevederile art. 5 alin. (1) lit. a) raportat la art. 6 alin. (1) din Regulamentul (UE) 2016/679, deoarece personalul Direcției Generale de Poliție Locală, aflat în exercitarea misiunilor și activităților specifice, a prelucrat date cu caracter personal prin utilizarea sistemului audio-video portabil de tip "Body-Worn Camera" (imagine și voce), fără să existe o obligație legală a operatorului și fără îndeplinirea vreunei alte condiții prevăzute la art. 6 alin. (1) din Regulamentul (UE) 2016/679, deși operatorul avea obligația de a prelucra datele în mod legal, echitabil și transparent față de persoana vizată.

Fapta constituie contravenția prevăzută de art. 14 alin. (5) lit. a) din Legea nr. 190/2018 și a fost sancționată cu avertisment - pentru încălcarea art. 5 alin. (1) lit. a) raportat



la art. 6 alin. (1) din Regulamentul (UE) 2016/679, contravențiile prevăzută de art. 14 alin. (5) lit. a) din Legea nr. 190/2018.

Avertismentul a fost însoțit de următoarele măsuri, menționate în planul de remediere anexat la procesul-verbal: să asigure conformitatea operațiunilor de prelucrare, efectuate prin utilizarea sistemelor audio-video portabile de tip "Body-Worn Camera", cu dispozițiile art. 5 și art. 6 din Regulamentul (UE) 2016/679.

Ulterior, în considerarea prevederilor art. 16 alin. (6) din Legea nr. 102/2005 republicată, a fost emisă Decizia nr. 4/19.01.2021, pe baza constatărilor din procesul-verbal menționat anterior, prin care s-a dispus ca operatorul să înceteze orice operațiune sau set de operațiuni de prelucrare de date cu caracter personal efectuate prin intermediul sistemelor audio-video de tip "Body -Worn Camera" și să șteargă sistemul de evidență a datelor cu caracter personal constituit ca urmare a utilizării unor astfel de sisteme.

Operatorul a contestat în instanță decizia emisă de Autoritatea națională de supraveghere.

Analizând probatoriul administrat în cauză, Tribunalul București, Secția a II-a Contencios Administrativ și Fiscal, a respins acțiunea formulată de reclamant ca neîntemeiată.

În mod corect instanța de fond a concluzionat că:

"decizia (...) este legală și temeinică, pârâta fiind obligată să o emită potrivit art. 16 alin. 6 din Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, citat mai sus."

Curtea de Apel București a respins ca nefondat apelul formulat de operator.

În mod corect, Curtea de Apel București a apreciat că decizia (...) emisă de către pârâtă este consecința întocmirii procesului-verbal de constatare/sanționare (...), pârâta fiind obligată să o emită potrivit dispozițiilor art. 16 alin. 6 din Legea nr. 102/2005.

De asemenea, instanța a constatat că „(...) susținerea reclamantei nu pot fi acceptate, deoarece Decizia contestată este motivată atât în drept, cât și în fapt. În consecință, prin Decizia contestată s-a impus reclamantei "să înceteze orice operațiune sau set de operațiuni de prelucrare de date cu caracter personal efectuate prin intermediul sistemelor audio-video de tip "Body-Worn Camera" și să șteargă sistemul de evidență a datelor cu caracter personal constituit ca urmare a realizării unor astfel de sisteme."



Pe cale de consecință, Curtea de Apel București a confirmat corectitudinea măsurilor dispuse prin decizia de ștergere emisă de instituția noastră.

Hotărârea judecătorească, favorabilă Autorității naționale de supraveghere, a rămas definitivă.

Secțiunea a 4-a: Informare publică

Autoritatea națională de supraveghere a continuat, în anul 2022, activitățile de comunicare destinate informării publicului larg, cu privire la regulile de prelucrare a datelor cu caracter personal, în contextul Regulamentului (UE) 2016/679, inclusiv în mediul on-line.

Astfel, prezentăm succint cele mai relevante dintre aceste manifestări:

→ Ziua Europeană a Protecției Datelor – 28 Ianuarie 2022

Ziua Europeană a Protecției Datelor a fost sărbătorită în data de 28 ianuarie 2022, de către toate statele membre ale Consiliului Europei și o marcat împlinirea a 41 de ani de la adoptarea, în anul 1981, la Strasbourg, a Convenției 108 pentru protecția persoanelor referitoare la prelucrarea automatizată a datelor cu caracter personal.

Prin Legea nr. 290 din 9 decembrie 2021, România a ratificat Protocolul de amendare a Convenției 108, deschis spre semnare la data de 10 octombrie 2018 la Strasbourg și semnat de țara noastră pe data de 26 iunie 2020.

Marcarea acestei zile a constituit un prilej de a aduce în atenția publicului importanța respectării principiilor de prelucrare a datelor cu caracter personal, a dreptului la viață privată și a dreptului la protecția datelor personale, consacrate ca drepturi fundamentale.

Pentru celebrarea Zilei Europene a Protecției Datelor, pe data de 28 ianuarie 2022, instituția noastră a organizat **Conferința on-line intitulată „Principalele aspecte constatate în activitatea Autorității naționale de supraveghere”**, în care s-au prezentat și dezbătut aspecte specifice de aplicare a regulilor de prelucrare a datelor personale. La acest eveniment au fost invitate, în principal, autoritățile și instituțiile publice



centrale reprezentative, cele mai importante asociații și uniuni profesionale, camere de comerț, companii și reprezentanți mass-media.

Cu această ocazie a fost lansat și **Ghidul privind prelucrările de date efectuate de asociațiile de proprietari**, pregătit de instituția noastră și destinat să lămurască aspecte specifice acestei categorii de operatori.

De asemenea, ca în fiecare an, Autoritatea națională de supraveghere a pregătit și pus la dispoziția publicului, pe pagina proprie de internet www.dataprotection.ro, **materialele informative (broșuri, pliante)** dedicate Zilei Europene a Protecției Datelor, precum și informații sintetice privind activitatea din anul anterior.

Totodată, pe postul național de televiziune TVR și în mijloacele de transport ale Societății de Transport București, a fost difuzat **clipul informativ** dedicat Regulamentului (UE) 2016/679 – mesaj de interes public, referitor la principalele aspecte reglementate de Regulamentul (UE) 2016/679, realizat de instituția noastră.

♦ **Eveniment aniversar - patru ani de la aplicarea Regulamentului (UE) 2016/679 – 25 Mai 2022**

Cu prilejul sărbătoririi a patru ani de la aplicarea Regulamentului (UE) 2016/679, a fost postat pe site-ul instituției un comunicat de presă ce prezintă o sinteză a celor mai semnificative aspecte din activitatea Autorității naționale de supraveghere, desfășurată pe parcursul primelor patru luni ale anului 2022, aspect ce relevă faptul că autoritatea a continuat activitatea de monitorizare și control cu privire la legalitatea prelucrărilor de date personale.

♦ **Acțiuni de informare destinate popularizării regulilor de protecție a datelor cu caracter personal.**

Autoritatea națională de supraveghere a elaborat „**Ghidul privind prelucrările de date efectuate de asociațiile de proprietari**”, ce cuprinde lămuriri referitoare la aplicarea adecvată a reglementărilor din domeniul protecției datelor cu caracter personal de către asociațiile de proprietari, acesta fiind transmis către Federația Asociațiilor de proprietari



din România și postat pe site-ul Autorității naționale de supraveghere www.dataprotection.ro.

♦ **Conferințe, seminarii, reuniuni**

Instituția noastră a participat activ și în anul 2022 la **reuniuni** cu incidență în domeniul protecției datelor, organizate de diverse instituții publice sau de entități private.

În cadrul acestor evenimente, reprezentanții Autorității naționale de supraveghere au clarificat anumite aspecte privind condițiile utilizării datelor, respectarea drepturilor persoanelor vizate, asigurarea confidențialității și protecției datelor cu caracter personal, ceea ce reflectă continuitatea deschiderii către societatea civilă.

În acest context, menționăm că Autoritatea națională de supraveghere a participat la o serie de **conferințe și seminarii**, cum ar fi:

• “Conferința Națională de Confidențialitate și Protecția Datelor PRIVACY ROMANIA”, în cadrul căreia a fost prezentat, un *“Scut bilanț al sancțiunilor cu amendă” acordate de Autoritatea națională de supraveghere , raportat la tema “Ce impact a avut GDPR în România în ultimii 4 ani?”*

• Conferința Națională Protecția Datelor în Domeniul Sanitar (CNPDDS 2022), unde a avut loc un discuții aplicate între reprezentanții Autorității naționale de supraveghere și cei ai unor companii private cu privire la prelucrări de date efectuate de operatorii din domeniul sanitar din România.

• Conferința Data Protection Romania. DPO Lives, organizată on-line, unde s-au abordat probleme de drept și probleme practice, inclusiv evoluțiile înregistrate în protecția datelor.

• Webinarul On-line dedicat *“Zilei Responsabilității cu protecția datelor cu caracter personal”*, cu tema “Impactul crizei sanitare și a conflictelor armate asupra domeniului protecției datelor cu caracter personal”.

• GDPR Webinar: Noutăți, Provocări și Oportunități, unde s-au discutat următoarele subiecte: publicitatea on-line (decizia IAB Europe), Drepturile persoanelor vizate - dreptul de acces, balancing test (LIA), breșe de securitate.

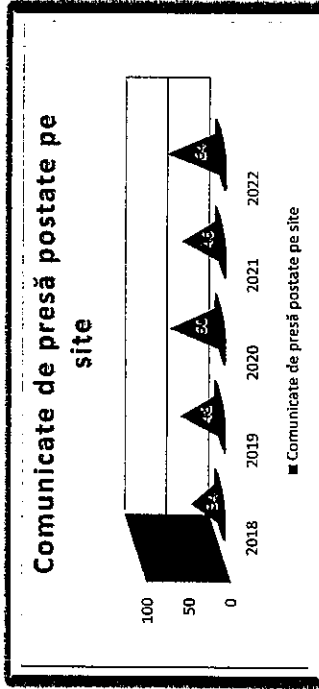
Pe de altă parte, subliniem că personalul instituției noastre a realizat o informare promptă și eficientă a operatorilor din mediul public și privat, precum și a persoanelor fizice, prin intermediul **audiențelor acordate la sediul** Autorității naționale de

supraveghere, dar și prin intermediul **consilierii telefonice**, în cadrul programului zilnic de relații cu publicul, cu privire la modalitatea de punere în practică a prevederilor Regulamentului (UE) 2016/679, fiind explicitate și clarificate o serie de măsuri pe care operatorii sunt obligați să le implementeze în vederea respectării dispozițiilor acestui Regulament.

În același timp, menționăm că Autoritatea națională de supraveghere a participat la reuniunile unor **grupuri de lucru interinstituționale**, în vederea discutării pe marginea unor proiecte de acte normative pe care le-au inițiat unele ministere, dar și pe diverse chestiuni complexe ce țin de protecția datelor personale.

♦ **Site-ul Autorității naționale de supraveghere**

Autoritatea națională de supraveghere a realizat și în cursul anului 2022 o informare promptă și eficientă cu privire la activitatea desfășurată, atât prin prisma celor **64 de comunicate de presă** postate pe site-ul instituției noastre la secțiunea „Știri”, cât și a informațiilor de la secțiunea specială dedicată Regulamentului (UE) 2016/679.

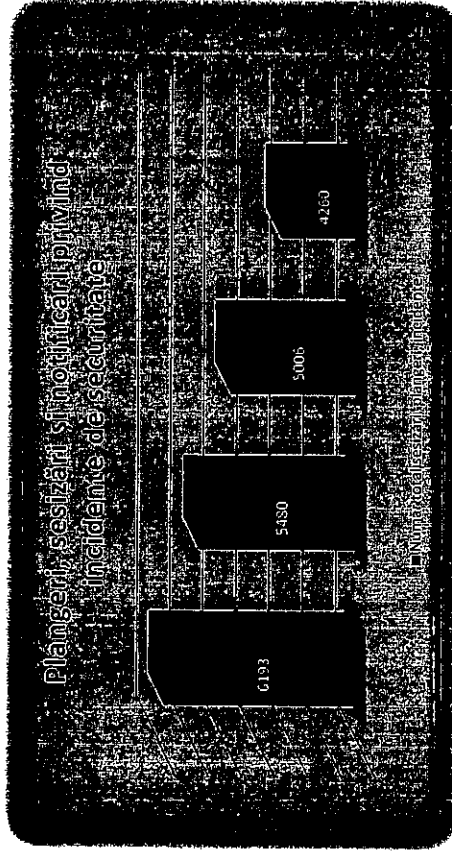


CAPITOLUL III

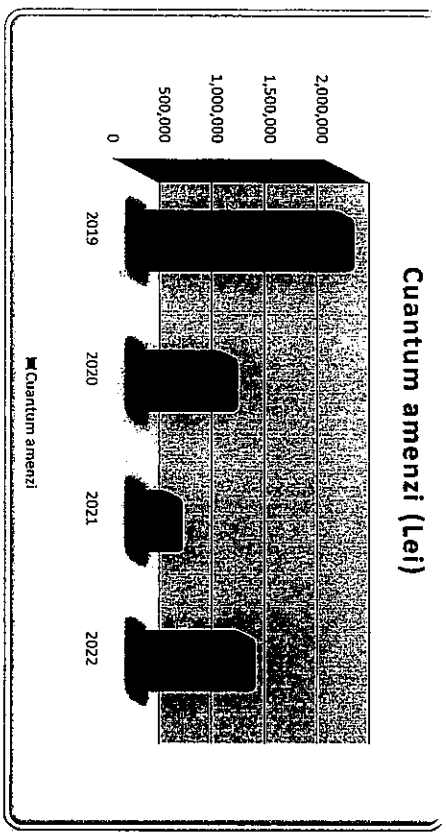
ACTIVITATEA DE MONITORIZARE ȘI CONTROL

Secțiunea 1: Prezentare generală

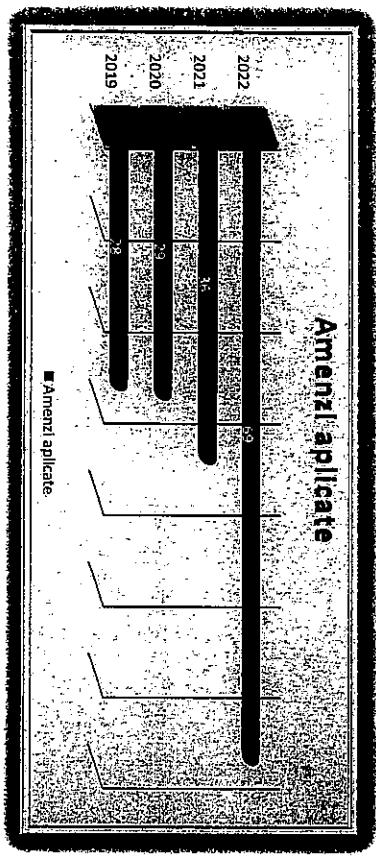
În cursul anului 2022, Autoritatea națională de supraveghere a primit un număr de **4260 de plângeri, sesizări și notificări privind incidente de securitate**, pe baza cărora au fost deschise **629 investigații**.



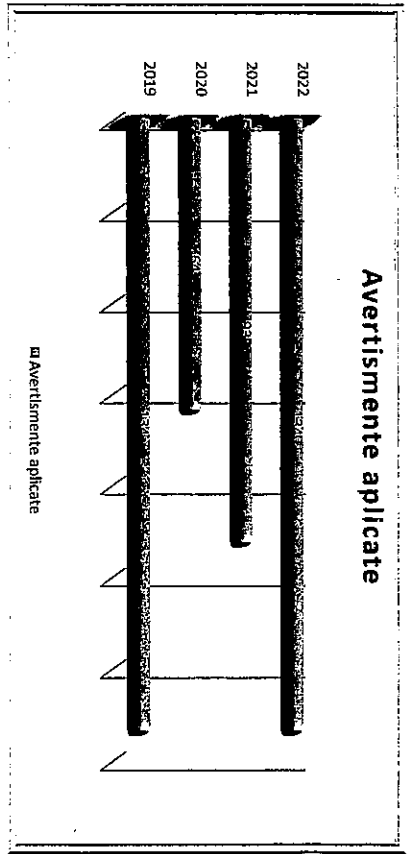
Ca urmare a investigațiilor, în anul 2022 au fost aplicate **amenzi în cuantum total de 1.058.863 lei**.



Astfel, ca urmare a investigațiilor, au fost aplicate **69** de amenzi.



De asemenea, au mai fost aplicate **134** de avertismente și au fost dispuse **93** de măsuri corective.



În anul 2022, **plângerile** înregistrate la Autoritatea națională de supraveghere au vizat, în principal, următoarele aspecte:

- prelucrarea datelor cu caracter personal cu încălcarea prevederilor art. 6 din Regulamentul (UE) 2016/679;
- încălcarea drepturilor persoanelor vizate, în special, a dreptului de acces al persoanei vizate și a dreptului la ștergerea datelor acestuia;
- încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date cu caracter personal.

Prin intermediul **sesizărilor** transmise în anul 2022 au fost semnalate, în principal, aspecte referitoare la:

- încălcarea principiilor prevăzute de Regulamentul (UE) 2016/679;
- dezvăluirea datelor cu caracter personal fără consimțământul persoanelor vizate;
- publicarea/dezvăluirea datelor cu caracter personal în mediul on-line, în special pe rețelele sociale;
- prelucrarea imaginilor prin intermediul sistemelor de supraveghere video;

- încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date personale prin neadaptarea de către operatori a măsurilor tehnice și organizatorice adecvate privind asigurarea securității prelucrărilor.

Referitor la **incidentele de securitate** transmise notificate de operatorii de date, acestea au vizat în anul 2022, în principal, următoarele aspecte:

- confidențialitatea, disponibilitatea, integritatea datelor cu caracter personal afectate în special ca urmare a dezăluirilor neautorizate
- accesul neautorizat la sistemele de supraveghere video cu circuit închis (CCTV)
- dezăluirea de date cu caracter personal pe internet
- dezăluirea de date cu caracter personal în sistemul medical
- accesul ilegal la datele cu caracter personal ale clienților din sistemul bancar.

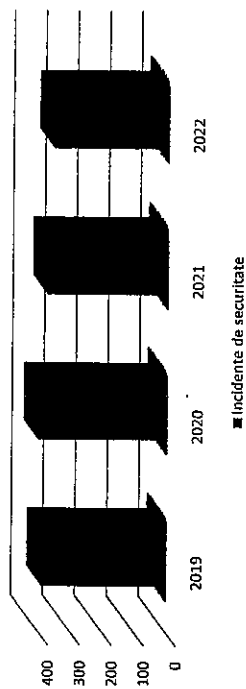
Secțiunea a 2-a: Investigații din oficiu

I. Prezentare generală

În cursul anului 2022, a continuat activitatea de monitorizare și control a operatorilor din sectorul public și privat, urmărindu-se cu prioritate obiective legate de respectarea prevederilor Regulamentului (UE) 2016/679, ale Legii nr. 190/2018, dar și ale Legii nr. 506/2004.

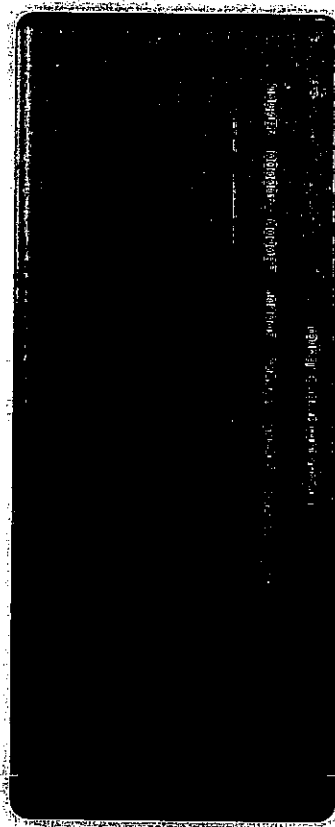
În anul 2022, Autoritatea națională de supraveghere a primit un număr total de **353** sesizări și notificări de încălcare a securității datelor cu caracter personal, dintre care **198 sesizări și 155 încălcări de securitate a datelor cu caracter personal**.

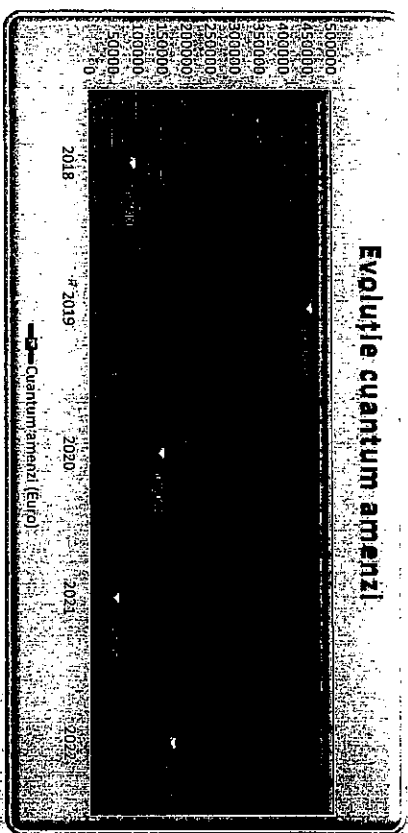
Notificări cu privire la încălcări de securitate și sesizări



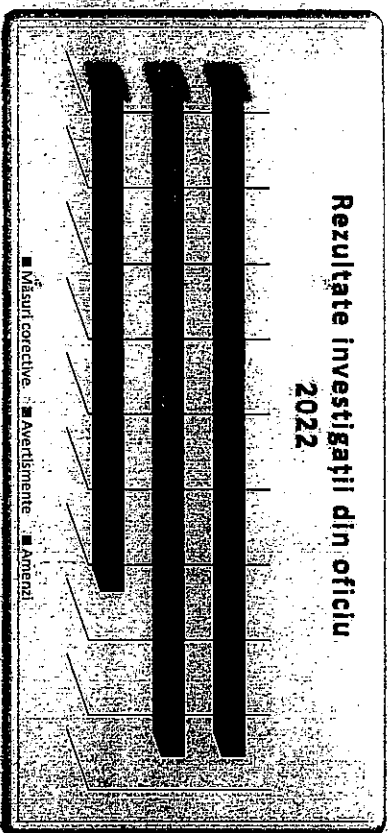
Pe baza sesizărilor și notificărilor de încălcare a securității datelor cu caracter personal au fost demarate **investigații** într-un număr de **314** cazuri.

Ca urmare a investigațiilor din oficiu efectuate au fost aplicate **44** amenzi în cuantum total de 160.090 Euro.





De asemenea, în investigațiile din oficiu efectuate au fost aplicate **44 avertismente** și au fost dispuse **33 măsuri corective**.



În anul 2022, prin intermediul sesizărilor transmise au fost semnalate, în principal, aspecte referitoare la:

- încălcarea principiilor legate de prelucrarea datelor cu caracter personal prevăzute de Regulamentul (UE) 2016/679;
- dezvăluirea datelor cu caracter personal fără consimțământul persoanelor vizate;

- publicarea/dezvăluirea datelor cu caracter personal în mediul on-line, în special pe rețelele sociale;
- prelucrarea imaginilor prin intermediul sistemelor de supraveghere video;
- încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date personale prin neadaptarea de către operatorii a măsurilor tehnice și organizatorice adecvate privind asigurarea securității prelucrărilor;
- prelucrarea datelor cu caracter personal cu încălcarea condițiilor privind legalitatea prelucrării.

Referitor la încălcarea securității datelor cu caracter personal, în cursul anului 2022, notificările transmise Autorității naționale de supraveghere au vizat, în principal, următoarele aspecte:

- confidențialitatea, disponibilitatea, integritatea datelor cu caracter personal afectate în special ca urmare a dezvăluirilor neautorizate;
- accesul neautorizat la sistemele de supraveghere video cu circuit închis (CCTV) sau dezvăluirea acestora;
- dezvăluirea de date cu caracter personal în sistemul medical;
- accesul ilegal la datele cu caracter personal ale clienților din sistemul bancar;
- divulgarea și accesul neautorizat la datele cu caracter personal ca urmare a unor atacuri informatice de tip ransomware.

Măsurile corective dispuse în urma investigațiilor din oficiu au vizat, în special, următoarele:

- punerea în aplicare a unor măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător, cum ar fi verificarea periodică, prin sondaj, a datelor înregistrate în aplicațiile informatice, pentru a identifica accesările neautorizate;
- instruirea personalului cu privire la măsurile luate de operator, astfel ca utilizatorii să aibă acces numai la datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu;



- revizuirea și actualizarea măsurilor tehnice și organizatorice implementate, ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, a procedurilor de lucru privind prelucrarea datelor cu caracter personal, precum și implementarea unor măsuri privind instruirea periodică a persoanelor care acționează sub autoritatea operatorului;
- asigurarea conformității operațiunilor de prelucrare cu dispozițiile Regulamentului (UE) 2016/679 și respectarea principiilor de prelucrare a datelor cu caracter personal;
- implementarea unor soluții informatice suplimentare de securizare a datelor și a unor politici de complexitate și expirare a parolelor.

A. Investigații referitoare la prelucrarea datelor cu caracter personal de către autorități și instituții publice

În cursul anului 2022, investigațiile din oficiu referitoare la prelucrarea datelor cu caracter personal de către autoritățile și instituțiile publice au avut ca obiect, în principal, divulgarea neautorizată și/sau accesul neautorizat la datele cu caracter personal, inclusiv pe pagina de web sau pe rețelele de socializare, încălcarea măsurilor de securitate și confidențialitate, precum și prelucrarea excesivă a datelor cu caracter personal raportat la scopul prelucrării.

Ca urmare a investigațiilor efectuate au fost aplicate atât sancțiuni contravenționale, cât și măsuri corective.

Măsurile corective dispuse în urma investigațiilor au vizat, în special, următoarele:

- revizuirea și actualizarea măsurilor tehnice și organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv a procedurilor de lucru referitoare la protecția datelor cu caracter personal, precum și realizarea unei instruiți pentru persoanele autorizate să prelucreze date asupra riscurilor și consecințelor pe care le implică divulgarea datelor personale;

- asigurarea conformității operațiunilor de prelucrare cu dispozițiile Regulamentului (UE) 2016/679;

- respectarea principiilor de prelucrare a datelor;



- instruirea personalului cu privire la măsurile luate de operator, astfel ca utilizatorii să aibă acces numai la datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu.

În majoritatea cazurilor, autoritățile publice au îndeplinit măsurile corective dispuse, în termenul acordat de Autoritatea națională de supraveghere.

1. FIȘĂ DE CAZ – Divulgarea neautorizată a datelor cu caracter personal pe site-ul unei autorități publice

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că pe site-ul unei autorități publice au fost postate mai multe fișiere ce conțin datele de identificare ale unor persoane fizice și tratamentul medical urmat de către acestea, iar macheta cu medicamentele eliberate pentru fiecare persoană putea fi descărcată de pe site-ul autorității publice respective.

Ulterior sesizărilor transmise, operatorul a notificat Autoritatea națională de supraveghere prin completarea formularului privind încălcarea securității datelor cu caracter personal, aprobat prin Decizia nr. 128/2018 privind aprobarea formularului tipizat al notificării de încălcare a securității datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679. Notificarea a avut ca obiect încălcarea securității datelor cu caracter personal prin divulgarea neautorizată pe site a mai multor fișiere ce conțineau datele de identificare ale persoanelor fizice și tratamentul medical urmat de către acestea.

Din investigația efectuată în acest caz, a reieșit că, pe site-ul autorității publice, în secțiunea destinată informațiilor pentru furnizori, erau încărcate mai multe fișiere în format *csv, arhivate zip și parolate, care conțineau următoarele date cu caracter personal: CNP persoană asigurată, tipul/categoria de asigurat - salariat, pensionar, copil etc., serie/nr. rețetă decontată, dată eliberare rețetă, valoare rețetă, valoarea compensată a rețetei, cod medicament/substanță activă, tip diagnostic etc. Parolele pentru accesarea fișierelor, comunicate individual fiecărui reprezentant legal al furnizorilor/companii farmaceutice, se aflau chiar în interiorul arhivelor pe care ar fi trebuit să le protejeze, fiind CUI-ul companiei farmaceutice.

Autoritatea națională de supraveghere a constatat în investigația efectuată în acest caz că operatorul investigat nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării. Aceasta a condus



la accesarea neautorizată a unor fișierelor arhivate (.zip) care conținneau informații precum CNP persoană asigurată, tipul/categoria de asigurat - salariat, pensionar, copil etc., serie/nr. rețea/decontată, dată eliberare rețea, valoare rețea, valoarea compensată a rețetei, cod medicament/substanță activă, tip diagnostic etc., de către o persoană care a utilizat o parolă de acces, divulgată de către una dintre farmaciile cărora i-au fost comunicate aceste informații în vederea realizării accesului, fiind afectate de incident 100.000 persoane fizice vizate.

Autoritatea națională de supraveghere a sancționat operatorul cu avertisment pentru încălcarea prevederilor art. 32 alin. (1) lit. b) și alin. (2) din Regulamentul (UE) 2016/679. Sancțiunea avertismentului a fost însoțită de aplicarea unor măsuri corective, prin planul de remediere, potrivit dispozițiilor art. 12 - 14 din Legea nr. 190/2018.

Astfel, în sarcina operatorului s-a dispus revizuirea și actualizarea măsurilor tehnice și organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv a procedurilor de lucru referitoare la protecția datelor cu caracter personal, precum și realizarea unei instruirii pentru persoanele autorizate să prelucreze date asupra riscurilor și consecințelor pe care le implică divulgarea datelor personale.

Datele cu caracter personal afectate de încălcarea de securitate au fost eliminate de pe site-ul operatorului investigat înainte de finalizarea investigației Autorității naționale de supraveghere.

2. FIȘĂ DE CAZ – Nerespectarea măsurilor dispuse prin planul de remediere de către o autoritate publică

Autoritatea națională de supraveghere a fost sesizată cu privire la o posibilă încălcare a dispozițiilor Regulamentului (UE) 2016/679 din cauza faptului că, la nivelul unei autorități publice, înregistrările din sistemul de supraveghere video au fost utilizate în scopul realizării pontajului angajaților.

Ca urmare a investigației efectuate în acest caz, s-a constatat că autoritatea publică în cauză a prelucreat datele cu caracter personal ale angajaților proprii într-un alt scop (întocmirea pontajului) decât scopul declarat al prelucrării („paza obiectivelor, bunurilor, valorilor și protecția persoanelor”), fără să existe o obligație legală a operatorului și fără îndeplinirea vreunei alte condiții prevăzute la art. 6 alin. (1) din Regulamentul (UE) 2016/679.



S-a constatat că nu s-a respectat art. 5 alin. (1) lit. b) din același act normativ, care stabilește obligația operatorului de a colecta date cu caracter personal în scopuri determinate, explicite și legitime și de a nu le prelucra ulterior într-un mod incompatibil cu aceste scopuri.

Autoritatea națională de supraveghere a sancționat operatorul cu avertisment pentru încălcarea art. 5 alin. (1) lit. b) și art. 6 din Regulamentul (UE) 2016/679.

Sancțiunea avertismentului a fost însoțită de aplicarea unor măsuri corective, prin planul de remediere, dispunându-se asigurarea conformității cu dispozițiile Regulamentului (UE) 2016/679 a operațiunilor de prelucrare a datelor cu caracter personal, inclusiv a celor efectuate prin intermediul sistemului de supraveghere video, prin implementarea de măsuri tehnice și organizatorice ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor.

Deoarece operatorul investigat nu a transmis o dovadă a îndeplinirii măsurilor dispuse prin planul de remediere, Autoritatea națională de supraveghere a reluat investigația pentru a verifica îndeplinirea măsurilor corective.

Ca urmare a investigației efectuate, autoritatea publică a fost sancționată cu amendă în cuantum de 13.000 lei, pentru încălcarea prevederilor art. 14 alin. (7) coroborat cu art. 14 alin. (1) și art. 13 alin. (4) din Legea nr. 190/2018, deoarece nu a adus la îndeplinire în totalitate măsurile prevăzute în planul de remediere anexat procesului-verbal de contravenție încheiat de Autoritatea națională de supraveghere.

Ulterior, autoritatea publică a transmis informații privind modalitatea de îndeplinire a măsurilor dispuse prin planul de remediere emis de către Autoritatea națională de supraveghere.

3. FIȘĂ DE CAZ – Divulgarea neautorizată a datelor cu caracter personal de către o instituție publică de învățământ superior

O instituție publică de învățământ superior a notificat Autoritatea națională de supraveghere cu privire la producerea unui incident de încălcare a securității datelor cu caracter personal, prin completarea formularului privind încălcarea securității datelor cu caracter personal, aprobat prin Decizia nr. 128/2018. Aceasta a constatat în publicarea pe platforma internă on-line a instituției de învățământ, a datelor cu caracter personal a unui număr de 232 studenți, de către un cadru didactic.



Ca urmare a investigației efectuate în acest caz, Autoritatea națională de supraveghere a constatat că instituția publică de învățământ superior nu a luat măsuri pentru a asigura că orice persoană fizică care acționează sub autoritatea sa și care are acces la date cu caracter personal nu le prelucrează decât la cererea sa și nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării. Aceasta a condus la divulgarea neautorizată a datelor cu caracter personal a 232 de studenți (nume, prenume, cod numeric personal, data nașterii, prenumele tatălui, prenumele mamei, numărul de telefon), prin publicarea lor, de către un cadru didactic, pe platforma internă on-line a operatorului și accesul neautorizat la aceste date al tuturor studenților la programul educațional de licență anul II, din cadrul unei facultăți ce aparține instituției de învățământ superior.

Autoritatea națională de supraveghere a sancționat operatorul cu avertisment pentru încălcarea art. 32. alin. (1) lit. b) și alin. (2) și (4) din Regulamentul (UE) 2016/679.

Sancțiunea avertismentului a fost însoțită de aplicarea unei măsuri corective, prin planul de remediere, potrivit dispozițiilor art. 12 - 14 din Legea nr. 190/2018.

Astfel, în sarcina operatorului s-a dispus asigurarea conformității operațiunilor de prelucrare a datelor personale ale studenților cu dispozițiile Regulamentului (UE) 2016/679, astfel încât să se evite divulgarea datelor personale obținute de la aceștia, în afara situațiilor permise de lege, inclusiv prin instruirea regulată a persoanelor ce prelucrează date sub autoritatea operatorului.

Ulterior, operatorul investigat a comunicat Autorității naționale de supraveghere că a emis o decizie aplicabilă facultăților din cadrul instituției de învățământ superior, care prevede instrucțiuni referitoare la prelucrarea datelor cu caracter personal.

4. FIȘĂ DE CAZ - Divulgarea neautorizată a datelor cu caracter personal ale studenților de către o instituție publică de învățământ superior

Autoritatea națională de supraveghere a fost sesizată cu privire la prelucrările de date cu caracter personal efectuate de către o instituție publică de învățământ superior pe site-ul propriu, prin afișarea unor tabele nominale cu datele personale și rezultatele obținute de studenți la admiterea la cursurile de licență, precum și cu privire la plasarea de cookies-uri fără consimțământul utilizatorilor și fără informarea prealabilă a acestora.



Ca urmare a investigației efectuate în acest caz, Autoritatea națională de supraveghere a constatat că instituția publică de învățământ superior a divulgat în mod excesiv și fără temei legal, tabele nominale conținând date cu caracter personal (nume, prenume, legitimații, opțiuni, medii bacalaureat, medii finală, programul de studii la care candidatul a fost admis) ale candidaților admisiși/respiși la diverse programe de studii din anul 2021.

Totodată, Autoritatea națională de supraveghere a constatat și faptul că operatorul nu a putut prezenta dovezi cu privire la obținerea consimțământului fără echivoc al utilizatorilor paginii de internet ce îi aparține, înainte de a permite stocarea de informații sau obținerea accesului la informația stocată în echipamentul terminal al utilizatorului, prin folosirea fișierelor de tip cookies.

Operatorul investigat a fost sancționat cu avertisment, pentru încălcarea prevederilor art. 5 alin. (1) lit. a) și c), prin raportare la dispozițiile art. 6 alin. (1) din Regulamentul (UE) 2016/679.

De asemenea, operatorul investigat a fost sancționat cu avertisment și pentru încălcarea art. 4 alin. (5) din Legea 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, modificată și completată, prin raportare la dispozițiile art. 6 alin. (1) lit. a) și art. 7 din Regulamentul (UE) 2016/679.

Sancțiunea avertismentului a fost însoțită de aplicarea unor măsuri corective, prin planul de remediere, potrivit dispozițiilor art. 12 - 14 din Legea nr. 190/2018.

Astfel, în sarcina operatorului s-a dispus revizuirea procedurilor interne și instruirea personalului propriu, pentru ca, în toate situațiile, datele personale să fie prelucrate în conformitate cu principiile de prelucrare prevăzute la art. 5 din Regulamentul (UE) 2016/679 și în baza unui temei legal stabilit potrivit art. 6 din Regulamentul (UE) 2016/679, astfel încât să nu fie prelucrate decât acele date personale care sunt necesare în vederea realizării scopurilor determinate, stabilite potrivit atribuțiilor legale ale instituției publice de învățământ superior.

Ca urmare a măsurilor dispuse prin procesul-verbal, operatorul a informat Autoritatea națională de supraveghere că:

- a șters de pe site-ul propriu tabelele nominale publicate;
- a revizuit operațiunile de prelucrare și a luat măsuri de adaptare a platformei electronice de admitere;

- a actualizat planul de instruire periodică a personalului;

- au fost aprobate modificări la Metodologia de admitere;

- a fost demarată procedura de achiziție și implementare a unei noi platforme de control și monitorizare a cookie-urilor care va permite utilizatorului retragerea acordului.

B. Investigații referitoare la prelucrarea datelor cu caracter personal de către entități din domeniul financiar-bancar

În anul 2022, investigațiile din oficiu la entitățile din domeniul financiar-bancar s-au desfășurat ca urmare a transmiterii notificărilor de încălcare a securității datelor cu caracter personal, precum și a sesizărilor cu privire la prelucrarea datelor cu caracter personal.

Notificările de încălcare a securității datelor cu caracter personal au avut ca obiect, în principal: divulgarea neautorizată și/sau accesul neautorizat la datele cu caracter personal prelucrate; neimplementarea unor măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, incluzând capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continuă ale sistemelor și serviciilor de prelucrare; neimplementarea unor măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului și care are acces la date cu caracter personal nu le prelucreează decât la cererea operatorului.

Sesizările au avut ca obiect, în principal, divulgarea neautorizată și/sau accesul neautorizat la datele cu caracter personal.

Ca urmare a investigațiilor efectuate au fost aplicate atât sancțiuni contravenționale, cât și măsuri corective.

1. FIȘĂ DE CAZ - Divulgarea neautorizată și accesul neautorizat la datele cu caracter personal ale clienților unei societăți bancare

O societate bancară a notificat Autoritatea națională de supraveghere cu privire la producerea mai multor incidente de încălcare a securității datelor cu caracter personal, prin completarea formularului privind încălcarea securității datelor cu caracter personal, aprobat prin Decizia nr. 128/2018.

Incidente de încălcare a securității datelor cu caracter personal notificate au constat în accesul neautorizat și/sau divulgarea neautorizată a datelor cu caracter personal

transmise, stocate sau prelucrate prin aplicațiile informatice utilizate de către societatea bancară în activitatea de creditare; divulgarea neautorizată a datelor cu caracter personal ale unor clienți către destinatari neautorizați, prin transmiterea la alte adrese de corespondență (e-mail, poștă) decât cele ale persoanelor vizate clienți, de către angajați ai societății bancare; accesul neautorizat la datele cu caracter personal ale clienților societății bancare și divulgarea neautorizată a acestor date de către angajați ai operatorului.

În urma investigațiilor efectuate, Autoritatea națională de supraveghere a constatat multiple încălcări ale dispozițiilor Regulamentului (UE) 2016/679, astfel:

- operatorul investigat nu a luat măsuri pentru a asigura că orice persoană fizică care acționează sub autoritatea operatorului și are acces la date cu caracter personal nu le prelucreează decât la cererea operatorului
- operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, incluzând capacitatea de a asigura confidențialitatea și integritatea sistemelor și serviciilor de prelucrare, precum și un proces pentru testarea, evaluarea și aprecierea perioade ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării
- operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, incluzând capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continuă ale sistemelor și serviciilor de prelucrare;
- operatorul investigat nu a pus în aplicare măsuri tehnice și organizatorice adecvate, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, destinate să pună în aplicare în mod eficient principiile de protecție a datelor și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele Regulamentului (UE) 2016/679 și a proteja drepturile persoanelor vizate.

Autoritatea națională de supraveghere a sancționat operatorul investigat, astfel:

- Amendă în cuantum de 98.980 lei (echivalentul a 20.000 EURO), pentru încălcarea art. 32 alin. (1) lit. b) și alin. (4), a art. 32 alin. (4) coroborat cu art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679;



- Avertisment, pentru încălcarea prevederilor art. 32 alin. (1) și art. 32 alin. (2) din Regulamentul (UE) 2016/679;
- Amendă în cuantum de 14.847 lei (echivalentul a 3.000 EURO), pentru încălcarea art. 32 alin. (4) coroborat cu art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679;
- Amendă în cuantum de 24.745 lei (echivalentul a 5.000 EURO), pentru încălcarea art. 25 alin. (1) din Regulamentul (UE) 2016/679;
- Avertisment, pentru încălcarea prevederilor art. 32 alin. (4) coroborat cu art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679.

Sanctiunile aplicate nu au fost contestate de operator.

2. FIȘĂ DE CAZ – Accesare neautorizată a datelor cu caracter personal ale clienților

O societate bancară a notificat Autoritatea națională de supraveghere cu privire la producerea unui incident de încălcare a securității datelor cu caracter personal, prin completarea formularului privind încălcarea securității datelor cu caracter personal, aprobat prin Decizia nr. 128/2018. Acesta a constat în accesarea neautorizată a datelor cu caracter personal din baza de date cu clienții, de către un angajat al societății, prin utilizarea necorespunzătoare a accesului acordat pentru îndeplinirea atribuțiilor sale de serviciu.

Autoritatea națională de supraveghere a constatat că operatorul investigat nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prezentat de prelucrare, generat în special, în mod accidental sau ilegal, de divulgarea neautorizată și accesul neautorizat la datele cu caracter. Aceasta a condus la divulgarea neautorizată și accesul neautorizat la datele cu caracter personal (date de identificare asociate actului de identitate, date de contact - număr de telefon și adresa de e-mail, date de natură bancară - informații referitoare la produsele deținute, tranzacțiile efectuate, informații de tip user și parolă din modulul de internet banking, precum și date asociate cardului bancar deținut) ale clienților operatorului investigat, deși potrivit art. 5 alin. (1) lit. f) din Regulamentul (UE) 2016/679, acesta avea obligația de a prelucra datele cu caracter personal într-un mod care asigură securitatea adecvată a acestora, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și



împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare ("integritate și confidențialitate").

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 98.076,00 lei (echivalentul a 20.000 EURO), pentru încălcarea art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679.

Sanctiunea aplicată nu au fost contestată de operator.

C. Investigații referitoare la prelucrarea datelor cu caracter personal de către entități din domeniul sănătății

În cursul anului 2022, sesizările și notificările încălcărilor de securitate cu privire la prelucrarea datelor cu caracter personal în domeniul sănătății, au avut ca obiect, în principal, divulgarea neautorizată și/sau accesul neautorizat la datele cu caracter personal ale persoanelor vizate (pacienți) prin transmiterea eronată a buletinelor de analize medicale/documente medicale sau ca urmare a neimplementării unor măsuri tehnice și organizatorice adecvate pentru ca orice persoană fizică care acționează sub autoritatea operatorului și care are acces la date cu caracter personal să nu le prelucreze decât la cererea operatorului.

Investigațiile efectuate de către Autoritatea națională de supraveghere au vizat prelucrarea datelor cu caracter personal, atât de către entități medicale din sectorul public (spitale), cât și entități medicale din sectorul privat.

Ca urmare a investigațiilor efectuate au fost aplicate atât sancțiuni contravenționale, cât și măsuri corective.

În majoritatea cazurilor, operatorii investigați au îndeplinit măsurile de remediere dispuse, în termenul acordat de Autoritatea națională de supraveghere.

1. FIȘĂ DE CAZ – Divulgarea și accesul neautorizat la datele cu caracter personal ale clienților unei societăți comerciale prin transmiterea eronată a contractelor de prestări servicii medicale

O societate comercială a notificat Autoritatea națională de supraveghere cu privire la producerea unui incident de încălcare a securității datelor cu caracter personal, prin

completarea formularului privind încălcarea securității datelor cu caracter personal, aprobat prin Decizia nr. 128/2018. Aceasta a constat în transmiterea eronată a unor acte adiționale ale contractelor de prestări servicii medicale, care conțineau date cu caracter personal ale unor clienți persoane fizice, ca atașamente la un e-mail transmis altui destinatar decât titularii datelor.

Ca urmare a investigației efectuate în acest caz, Autoritatea națională de supraveghere a constatat că societatea nu a luat măsuri pentru a se asigura că orice persoană fizică care acționează sub autoritatea operatorului și are acces la date cu caracter personal nu le prelucreează decât la cererea acestuia din urmă și nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, incluzând capacitatea de a asigura confidențialitatea și integritatea sistemelor și serviciilor de prelucrare.

Aceasta a condus la pierderea confidențialității datelor cu caracter personal prelucrate, prin divulgarea neautorizată și accesul neautorizat la datele cu caracter personal ale clienților (numele și prenumele, codul numeric personal, adresa din CI și semnătura persoanelor vizate), transmise altei persoane fizice decât destinatarul, prin intermediul e-mailului, deși avea această obligație potrivit art. 5 alin. (1) lit. f din Regulamentul (UE) 2016/679 – principiul "integritate și confidențialitate".

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 4.901 RON (echivalentul a 1.000 EURO), pentru încălcarea prevederilor art. 32 alin. (4) coroborat cu art. 32 alin. (1) lit. b) și alin. (2) din Regulamentul (UE) 2016/679.

2. **FIȘĂ DE CAZ – Transmitere eronată a datelor cu caracter personal privind starea de sănătate de către un laborator de analize medicale**

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că un laborator de analize medicale a transmis un buletin de analize, aparținând unui pacient, către alt pacient decât titularul datelor.

Din investigația efectuată în acest caz, a rezultat că o angajată a operatorului investigat a asociat în baza de date, în mod eronat, adresa de e-mail a unei paciente cu contul unui alt pacient. Aceasta a condus la divulgarea neautorizată și accesul neautorizat la

datele privind sănătatea ale unui pacient, prin transmiterea la o adresă de e-mail a altui pacient, asociată eronat în baza de date a operatorului.

Autoritatea națională de supraveghere a constatat că operatorul investigat nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prezentat de prelucrare și nu a luat măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea sa și care are acces la date cu caracter personal nu le prelucreează decât la cererea operatorului.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 24.143,50 lei (echivalentul a 5.000 EURO), pentru încălcarea art. 32 alin. (1), art. 32 alin. (2) și art. 32 alin. (4) din Regulamentul (UE) 2016/679.

Totodată, a fost dispusă și măsura corectivă constând în revizuirea și actualizarea măsurilor tehnice și organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv a procedurilor de lucru referitoare la protecția datelor cu caracter personal, precum și implementarea unor măsuri privind instruirea periodică a persoanelor care acționează sub autoritatea sa, referitor la obligațiile ce le revin conform prevederilor Regulamentul (UE) 2016/679, inclusiv cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcție de specificul activității.

Operatorul investigat a transmis Autorității naționale de supraveghere măsurile întreprinse cu privire la revizuirea măsurilor tehnice și organizatorice implementate, instruirea personalului propriu, precum și cu privire la revizuirea măsurilor tehnice și organizatorice implementate și a achitat amenda aplicată.

D. **Investigații referitoare la prelucrarea datelor cu caracter personal în domeniul comunicațiilor electronice**

În cursul anului 2022, sesizările și notificările încălcărilor de securitate cu privire la prelucrarea datelor cu caracter personal în domeniul comunicațiilor electronice au avut ca obiect, în principal, divulgarea neautorizată și/sau accesul neautorizat la datele cu caracter personal ca urmare a neimplementării unor măsuri tehnice și organizatorice adecvate riscului prezentat de prelucrare, precum și ca urmare a faptului că operatorul nu a luat măsuri pentru a asigura că orice persoană fizică care acționează sub autoritatea operatorului sau a



persoanei împuțernicite de operator și care are acces la datele cu caracter personal nu le prelucreează decât la cererea operatorului.

În urma investigațiilor efectuate au fost aplicate atât sancțiuni contravenționale, cât și măsuri corective.

În majoritatea cazurilor, operatorii investigați au îndeplinit măsurile de remediere dispuse, în termenul acordat de Autoritatea națională de supraveghere.

1. FIȘĂ DE CAZ – Divulgare neautorizată a datelor cu caracter personal pe o platformă de anunțuri imobiliare on-line

Autoritatea națională de supraveghere s-a sesizat din oficiu cu privire la o posibilă încălcare a securității datelor cu caracter personal pe o platformă de anunțuri imobiliare, în ceea ce privește posibilitatea accesării neautorizate a unor fișiere din baza de date a operatorului, prin introducerea adresei URL.

În urma investigației efectuate în acest caz, Autoritatea națională de supraveghere a constatat că operatorul investigat nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării generat în special, în mod accidental sau ilegal, de divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal stocate sau prelucrate într-un alt mod.

Aceasta a condus la pierderea confidențialității datelor cu caracter personal (nume, prenume, număr de telefon, adresa de e-mail, adresa poștală, cod numeric personal, semnătura, copii ale cărților de identitate, inclusiv coduri de identificare, funcție/calitate, date bancare, informații incluse în extrase de carte funciară/schițe cadastrale, titluri de proprietate, imagini de profil al utilizatorilor) ale unui număr de 194.309 persoane vizate, prin configurarea greșită a serviciului Amazon Web Services (AWS) Simple Storage Service (S3), de către un angajat al operatorului. Amazon Web Services (AWS) Simple Storage Service (S3) este un mediu de stocare în cloud, similar cu un folder de fișiere.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum 39.272 lei (echivalentul a 8.000 EURO), pentru încălcarea prevederilor art. 32 alin. (1) lit. b) și alin. (2) din Regulamentul (UE) 2016/679.



2. FIȘĂ DE CAZ – Prelucrarea nelegală a datelor cu caracter personal prin intermediul unui site

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că, pe site-ul unei societăți de transport, nu se regăsesc informații privind prelucrarea datelor cu caracter personal, inclusiv referitoare la drepturile persoanelor vizate și modul de exercitare a acestor drepturi, conform prevederilor Regulamentului (UE) 2016/679.

Că urmare a investigației efectuate în acest caz, operatorul nu a furnizat informațiile solicitate de către Autoritatea națională de supraveghere pentru îndeplinirea sarcinilor sale, cu încălcarea prevederilor art. 58 alin. (1) lit. a) și lit. e) din Regulamentul (UE) 2016/679.

S-a mai constatat că operatorul nu a asigurat o informare clară, completă și corectă a persoanelor vizate ale căror date cu caracter personal le prelucreează prin intermediul site-ului propriu, întrucât nu a oferit toate informațiile prevăzute de dispozițiile art. 12-22 din Regulamentul (UE) 2016/679, cum ar fi cele referitoare la scopul prelucrării și temeiul juridic, identitatea și datele de contact ale operatorului, perioada pentru care vor fi stocate datele sau criteriile utilizate pentru a stabili această perioadă, condițiile de exercitare a drepturilor.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 34.630,40 lei (echivalentul a 7.000 EURO), pentru încălcarea dispozițiilor art. 58 alin. (1) lit. a) și e) din Regulamentul (UE) 2016/679, precum și cu avertisment, pentru încălcarea dispozițiilor art. 12 alin. (1) din Regulamentul (UE) 2016/679.

Totodată, s-a dispus față de operator și măsura corectivă a asigurării informării persoanelor vizate prin comunicarea într-o formă concisă, transparentă, inteligibilă și ușor accesibilă a tuturor informațiilor prevăzute de art. 12 din Regulamentul (UE) 2016/679.

3. FIȘĂ DE CAZ – Dezvăluirea unor date cu caracter personal pe site-ul unei societăți comerciale

Autoritatea națională de supraveghere a fost sesizată cu privire la dezvăluirea, pe site-ul unei societăți comerciale, a datelor cu caracter personal ale persoanelor fizice, care au calitatea de foști angajați/șoferi ai altor societăți comerciale.

Din investigația efectuată în acest caz, a rezultat că operatorul investigat a prelucrat pe site-ul propriu, datele cu caracter personal (nume și prenume șofer, localitate și județ, anul lichidării, perioada angajării, incidente de natură specifică profesiei de șofer - furt de carburant, de marfă, de bani sau alte valori, accidente, amenzi din vină șoferului, consum de

alcool și probleme de comportament, tipuri de abilități - stil de șofat, întreținere mașină, abilități de lucru cu documente, punctualitate, atitudine, cunoștințe teoretice) ale unor persoane fizice/șoferi. Aceste date fuseseră colectate în mod indirect de la entități care dețineau un abonament pentru utilizarea aplicației, fără să existe o obligație legală a operatorului, fără consimțământul persoanelor vizate și fără îndeplinirea vreunei alte condiții prevăzute la art. 6 alin. (1) din Regulamentul (UE) 2016/679, deși operatorul avea obligația de a prelucra datele în mod legal, echitabil și transparent față de persoana vizată potrivit art. 5 alin. (1) lit. a) din Regulamentul (UE) 2016/679.

Autoritatea națională de supraveghere a mai constatat că operatorul investigat nu a luat toate măsurile necesare pentru a verifica exactitatea datelor cu caracter personal ale persoanelor fizice/șoferi, colectate în mod indirect prin intermediul aplicației de pe site-ul propriu, de la foști angajați (entități care dețineau un abonament pentru utilizarea aplicației), precum și pentru actualizarea datelor prelucrate.

Totodată, s-a constatat că operatorul investigat nu a făcut dovada că a luat măsuri adecvate pentru a furniza persoanelor vizate informațiile prevăzute la art. 14 din Regulamentul (UE) 2016/679, în condițiile de transparență menționate la art. 12 din același act normativ, referitor la prelucrarea datelor cu caracter personal pe site-ul propriu.

În urma investigației efectuate, Autoritatea națională de supraveghere a sancționat operatorul, astfel:

- Amendă în cuantum de 24.564,00 lei (echivalentul a 5.000 EURO) pentru încălcarea art. 6 alin. (1), coroborat cu art. 5 alin. (1) lit. a) din Regulamentul (UE) 2016/679;
- Avertisment, pentru încălcarea prevederilor art. 5 alin. (1) lit. d) din Regulamentul (UE) 2016/679;

- Avertisment, pentru încălcarea prevederilor art. 14, coroborat cu art. 12 din Regulamentul (UE) 2016/679.

De asemenea, s-a aplicat măsura corectivă de a asigura conformitatea operațiunilor de prelucrare efectuate cu dispozițiile art. 5 și art. 6 din Regulamentul (UE) 2016/679.

Totodată, Autoritatea națională de supraveghere a dispus, prin decizie, ștergerea datelor cu caracter personal din sistemul de evidență constituit ca urmare a prelucrării datelor cu caracter personal ale persoanelor fizice ce au calitatea de foști angajați/șoferi ai unor societăți comerciale, care dețin un abonament pentru utilizarea aplicației, pusă la dispoziție pe site-ul operatorului investigat.

Ca urmare a emiterii procesului-verbal și a deciziei privind ștergerea datelor cu caracter personal de către Autoritatea națională de supraveghere, operatorul investigat a oprit aplicația de pe site-ul propriu și a șters datele cu caracter personal colectate.

E. Investigații referitoare la prelucrarea datelor cu caracter personal, efectuată de către furnizorii de servicii

În anul 2022, Autoritatea națională de supraveghere a efectuat investigații din oficiu pentru soluționarea sesizărilor și încălcărilor de securitate a datelor cu caracter personal la diverși furnizori de servicii.

Încălcarea securității datelor cu caracter personal a constatat, în principal, în divulgarea și/sau accesul neautorizat la datele cu caracter personal, ca urmare a neimplementării măsurilor tehnice și organizatorice adecvate riscului prezentat de prelucrare, atât în calitate de operatori de date cu caracter personal, cât și în calitate de persoane împuternicite de către operator.

În urma investigațiilor efectuate au fost aplicate sancțiuni contravenționale și măsuri corective, atât operatorilor cât și împuterniciilor acestora.

1. FIȘĂ DE CAZ - Divulgarea neautorizată și accesul neautorizat la datele cu caracter personal ale clienților unui furnizor de energie

Un furnizor de energie a notificat Autoritatea națională de supraveghere cu privire la producerea a 5 incidente de încălcare a securității datelor cu caracter personal, prin completarea formularului aprobat prin Decizia nr. 128/2018.

Încălcările de securitate notificate au constatat în divulgarea neautorizată și accesul neautorizat la datele cu caracter personal ale clienților prin transmiterea eronată de contracte comerciale către alți clienți, respectiv ca urmare a unor deficiențe ale platformei online de contractare.

Au fost afectate, în principal, următoarele categorii de date cu caracter personal: nume, prenume, cod numeric personal, serie carte de identitate, nr. carte de identitate, dată emiterie carte de identitate, adresă de domiciliu declarată în cartea de identitate, date reprezentant, semnătură, e-mail, adresă loc de consum, adresă de corespondență, cod unic



de consum, cod client, nr. contract, nr. factură, serie factură, data emiterii, consum estimat lunar de energie electrică, POD, calitate în raport de dreptul de proprietate.

Autoritatea națională de supraveghere a constatat, în cadrul investigației efectuate în acest caz, faptul că operatorul nu a pus în aplicare măsuri tehnice și organizatorice adecvate, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, destinate să pună în aplicare în mod eficient principiile de protecție a datelor și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele Regulamentului (UE) 2016/679 și a proteja drepturile persoanelor vizate.

Totodată, a constatat că operatorul nu a luat măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea sa și care are acces la date cu caracter personal nu le prelucrează decât la cererea sa, precum și faptul că nu a luat măsurile necesare pentru a asigura că datele cu caracter personal inexacte sunt șterse sau rectificate fără întârziere, deși avea obligația de a prelucra date exacte și, în cazul în care este necesar, să fie actualizate.

Autoritatea națională de supraveghere a sancționat operatorul astfel:

- Amendă în cuantum de 34.500,20 lei (echivalentul a 7.000 EURO), pentru încălcarea prevederilor art. 25 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679;
- Amendă în cuantum de 14.785,20 lei (echivalentul a 3.000 EURO), pentru încălcarea prevederilor art. 32 alin. (4) coroborat cu art. 32 alin. (1) lit. b) și art. 32 alin. (2) din Regulamentul (UE) 2016/679;
- Avertisment, pentru încălcarea prevederilor art. 5 alin. (1) lit. d) din Regulamentul (UE) 2016/679.

Totodată, sancțiunile aplicate au fost însoțite și de măsuri corective, constând în revizuirea și actualizarea măsurilor tehnice și organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv implementarea unui proces pentru testarea, evaluarea și aprecierea periodică ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării, precum și implementarea unor măsuri privind instruirea periodică a persoanelor care acționează sub autoritatea sa, referitor la obligațiile ce le revin conform prevederilor Regulamentului (UE) 2016/679 și riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcție de specificul activității, respectiv identificarea și implementarea unor măsuri pentru a se asigura că datele cu caracter



personal prelucrate sunt exacte și actualizate, având în vedere scopurile pentru care sunt prelucrate, inclusiv în ceea ce privește evidența exercitării dreptului la ștergerea datelor cu caracter personal, de către persoanele vizate.

Operatorul investigat a comunicat Autorității naționale de supraveghere care au fost demersurile întreprinse de acesta ca urmare a măsurilor corective aplicate, în termenul stabilit în procesul-verbal de constatare/sancționare.

2. FIȘĂ DE CAZ – Divulgare neautorizată a datelor cu caracter personal de către o persoană împuternicită - furnizor de servicii poștale

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că baza de date a unui furnizor de servicii poștale este postată spre vânzare pe un site.

Din investigația efectuată în acest caz, a rezultat că datele cu caracter personal (număr și dată AWB – documentul de transport ce însoțește obligatoriu expedierea oricărui colet, indicative curieri, nume expeditor, nume și prenume destinatar, număr de telefon, adresă, status livrare, tipul serviciului, greutate colet, suma de încasat, intervalul de livrare), prelucrate de către furnizorul de servicii poștale, erau disponibile spre vânzare pe un forum și puteau fi vizualizate prin accesarea unui link, deși persoana împuternicită de către operator este obligată să ia toate măsurile necesare pentru a proteja sistematic prelucrarea datelor cu caracter personal ale persoanelor fizice, așa cum prevede art. 28 alin. (3) lit. c) din Regulamentul (UE) 2016/679, inclusiv împotriva divulgării și/sau accesului neautorizat la date.

Autoritatea națională de supraveghere a constatat că furnizorul de servicii poștale, în calitate de persoană împuternicită a două societăți comerciale, nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării pentru drepturile și libertățile persoanelor fizice, ceea ce a condus la divulgarea și/sau accesul neautorizat la datele cu caracter personal pentru un număr de 26.566 persoane fizice vizate. Totodată, s-a constatat că încălcarea securității datelor cu caracter personal a fost posibilă ca urmare a unei configurări greșite a serviciului Application gateway din Microsoft Azure.

Autoritatea națională de supraveghere a sancționat persoana împuternicită cu amendă în cuantum de 14.825.70 lei (echivalentul a 3.000 EURO), pentru încălcarea dispozițiilor art. 29, art. 32 alin. (1) lit. b) și alin. (2) din Regulamentul (UE) 2016/679.

3. FIȘĂ DE CAZ – Divulgare neautorizată a datelor cu caracter personal ale clienților unei companii de utilitate publică

O companie de utilitate publică a notificat Autoritatea națională de supraveghere cu privire la producerea unui incident de încălcare a securității datelor cu caracter personal, prin completarea formularului privind încălcarea securității datelor cu caracter personal, aprobat prin Decizia nr. 128/2018. Acesta a constat în divulgarea neautorizată a adreselor de e-mail pentru 4.500 de clienți ai companiei.

Ca urmare a investigației efectuate în acest caz, Autoritatea națională de supraveghere a constatat că, la transmiterea unui e-mail de informare privind opțiunea de primire a facturii electronice către utilizatorii înregistrați pe portalul on-line al companiei, s-au înscris, din eroare, adresele de e-mail ale clienților la secțiunea TO, în loc de BCC, astfel că, în momentul transmiterii mesajului, au fost divulgate neautorizat 4500 de adrese de e-mail.

S-a constatat deci că operatorul investigat nu a luat măsuri pentru a asigura că orice persoană fizică care acționează sub autoritatea sa și care are acces la date cu caracter personal nu le prelucreează decât la cererea sa și nici nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, incluzând capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare. Aceasta a condus la divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal (adresa de e-mail) ale unui număr semnificativ de clienți proprii, prin transmiterea unor mesaje electronice cu înscrisura adreselor de e-mail la secțiunea TO, în loc de BCC, deși operatorul avea obligația de a respecta prevederile art. 5 lit. f) din Regulamentul (UE) 2016/679.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 14.757,60 lei (echivalentul a 3.000 EURO), pentru încălcarea art. 32 alin. (4) coroborat cu art. 32 alin. (1) lit. b) și art. 32 alin. (2) din Regulamentul (UE) 2016/679.

F. Alte cazuri:

Prin intermediul sesizărilor transmise Autorității naționale de supraveghere au fost semnalate, în principal, aspecte referitoare la încălcarea principiilor legate de prelucrarea datelor cu caracter personal, prevăzute de Regulamentul (UE) 2016/679; dezvăluirea datelor

cu caracter personal fără conștințământul persoanelor vizate; publicarea/dezvăluirea datelor cu caracter personal în mediul on-line, în special pe rețelele sociale; prelucrarea imaginilor prin intermediul sistemelor de supraveghere video; încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date personale prin neadaptarea de către operatorii a măsurilor tehnice și organizatorice adecvate privind asigurarea securității prelucrărilor; prelucrarea datelor cu caracter personal cu încălcarea condițiilor privind legalitatea prelucrării.

În ceea ce privește încălcările de securitate a datelor cu caracter personal notificate de către entitățile din domeniul public și privat, acestea au constat, în principal, în nerespectarea prevederilor art. 32 din Regulamentul (UE) 2016/679 și au fost generate de neimplementarea de măsuri tehnice și organizatorice adecvate, precum și de faptul că operatorul nu a luat măsuri pentru a asigura că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei impunerice de operator și care are acces la datele cu caracter personal nu le prelucreează decât la cererea operatorului, ceea ce a condus la divulgarea sau accesul neautorizat la datele cu caracter personal prelucrate.

Totodată, încălcările de securitate au fost generate și de neimplementarea unor măsuri tehnice și organizatorice adecvate, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, cum ar fi pseudonimizarea, destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate.

De asemenea, în cadrul investigațiilor efectuate s-a constatat că operatorii nu au pus în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării și nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane.

Ca urmare a investigațiilor efectuate au fost aplicate atât sancțiuni contravenționale cu amendă și avertisment, cât și măsuri corective.

În majoritatea cazurilor, operatorii investigați au îndeplinit măsurile de remediere dispuse, în termenul acordat de Autoritatea națională de supraveghere.



1. FIȘĂ DE CAZ – Accesul neautorizat la datele cu caracter personal din dosarele de personal ale angajaților unei societăți comerciale

O societate comercială a notificat Autoritatea națională de supraveghere cu privire la producerea unui incident de încălcare a securității datelor cu caracter personal, prin completarea formularului aprobat prin Decizia nr. 128/2018. Aceasta a constat în sustragerea, de către persoane neautorizate, a unui biblioraft conținând dosarele de personal a 12 angajați ai societății și accesul neautorizat la acestea.

Autoritatea națională de supraveghere a constatat în cadrul investigației efectuate că operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării. Aceasta a condus la accesarea neautorizată a datelor cu caracter personal a angajaților operatorului investigat, prin sustragerea unui biblioraft, conținând dosarele de personal a 12 angajați.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 9.828,00 lei (echivalentul a 2.000 EURO) pentru încălcarea art. 32 alin. (1) lit. b) și art. 32 alin. (2) din Regulamentul (UE) 2016/679.

De asemenea, în temeiul art. 58 alin. (2) lit. d) din Regulamentul (UE) 2016/679, raportat la art. 14 alin. (1) și art. 16 alin. (5) din Legea nr. 102/2005, s-a dispus și măsura corectivă privind revizuirea și actualizarea măsurilor tehnice și organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv a procedurilor de lucru referitoare la protecția datelor cu caracter personal, precum și realizarea unei instruirii pentru persoanele autorizate să prelucreze date asupra riscurilor și consecințele pe care le implică divulgarea datelor personale.

2. FIȘĂ DE CAZ – Divulgarea și accesul neautorizat la datele cu caracter personal ca urmare a unui atac informatic de tip ransomware

O societate comercială a notificat Autoritatea națională de supraveghere cu privire la producerea a două incidente de încălcare a securității datelor cu caracter personal, prin completarea formularului aprobat prin Decizia nr. 128/2018. Acestea au constat în divulgarea și accesul neautorizat asupra site-ului operatorului, respectiv asupra infrastructurii IT a acestuia, ca urmare a unui atac informatic de tip ransomware.

Din investigația efectuată în acest caz a rezultat că, urmare a postării pe un forum public a unui fișier care conținea baza de date a clienților operatorului investigat, acesta a



identificat pe serverul intern niște fișiere cu extensii suspecte și a constatat că sistemele sale interne au suferit un atac informatic de tip ransomware. Totodată, informațiile existente pe serverele interne ale operatorului au fost criptate și a fost transmis un mesaj de răscumpărare, în sensul decriptării datelor pentru anumite beneficii financiare.

Autoritatea națională de supraveghere a constatat că operatorul investigat nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prezentat de prelucrare. Aceasta a condus la divulgarea neautorizată a datelor cu caracter personal (nume, prenume, număr de telefon, email, parola sub formă criptată, adresa IP de pe care a fost creat contul de utilizator), ale unui număr de 10.739 clienți, fiind postată pe un forum public o bază de date care conținea în denumire numele operatorului și la accesul neautorizat și pierderea integrității și disponibilității datelor cu caracter personal pentru aproximativ 100 persoane vizate (nume, prenume, CNP-uri și parolele conturilor din sistemul de concedii ale companiei ale angajaților, adresele poștale, numele, prenumele, adresele de email, CNP-urile și datele din cărțile de identitate ale unor traducători).

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 24.566 lei (echivalentul a 5.000 EURO), pentru încălcarea prevederilor art. 32 alin. (1) lit. b) și c) și art. 32 alin. (2) din Regulamentul (UE) 2016/679.

Totodată, sancțiunea aplicată a fost însoțită de măsura corectivă constând în revizuirea și actualizarea măsurilor tehnice și organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, a procedurilor de lucru referitoare la protecția datelor cu caracter personal, inclusiv implementarea unor soluții informatice suplimentare de securizare a datelor și a unor politici de complexitate și expirare a parolilor.

Operatorul investigat a comunicat Autorității naționale de supraveghere demersurile întreprinse de acesta pentru îndeplinirea măsurii corective, în termenul stabilit în procesul-verbal de constatare/sancționare.



3. FIȘĂ DE CAZ – Divulgarea neautorizată a datelor cu caracter personal a clienților unei societăți comerciale, pe site-ul personal al unui angajat

Autoritatea națională de supraveghere a fost sesizată cu privire la divulgarea pe un site a unui tabel centralizator, care conținea date cu caracter personal ale unor clienți ai unei societăți comerciale, precum și ale partenerilor de viață ai acestora.

Din investigația efectuată în acest caz, a reieșit că o persoană fizică, angajat al societății comerciale, a divulgat pe pagina de internet personală, accesibilă public, o evidență în format Excel (tabel structurat), care conține date cu caracter personal (nume, prenume, CNP, număr telefon, serie și nr. CI, adresă de e-mail, date bancare, achiziții de imobile, stare civilă, sumă solicitată, bancă, observații) ale clienților și partenerilor de viață ai clienților societății la care era angajat.

Autoritatea națională de supraveghere a constatat că persoana fizică, în calitate de operator de date cu caracter personal, a divulgat, pe pagina de internet personală, date cu caracter personal, fără consimțământul persoanelor vizate și fără îndeplinirea vreunei alte condiții prevăzute la art. 6 alin. (1) din Regulamentul (UE) 2016/679, deși potrivit art. 5 alin. (1) lit. a) din Regulamentul (UE) 2016/679, operatorul avea obligația de a prelucra datele în mod legal, echitabil și transparent față de persoanele vizate.

Autoritatea națională de supraveghere a sancționat operatorul - persoană fizică cu amendă în cuantum de 493,91 lei (echivalentul a 100 EURO), pentru încălcarea art. 5 alin. (1) lit. a) și lit. f) și art. 6 alin. (1) lit. a) din Regulamentul (UE) 2016/679.

Totodată, deoarece nu a furnizat toate informațiile solicitate de către Autoritatea națională de supraveghere pentru îndeplinirea sarcinilor sale, operatorul - persoană fizică a fost sancționat cu 246,95 lei (echivalentul a 50 EURO), pentru încălcarea dispozițiilor art. 58 alin. (1) lit. a) și e) din Regulamentul (UE) 2016/679.

În ceea ce privește prelucrarea datelor cu caracter personal de către societatea comercială angajatoare a persoanei fizice care a divulgat pe pagina de internet personală, un tabel cu datele personale ale clienților și partenerilor de viață ai clienților societății angajatoare, Autoritatea națională de supraveghere a demarat o investigație din oficiu.

Ca urmare a investigației efectuate în acest caz, Autoritatea națională de supraveghere a constatat că societatea comercială nu a luat măsuri adecvate pentru a se asigura faptul că



office persoană fizică care acționează sub autoritatea sa și care are acces la date cu caracter personal nu le prelucrează decât la cererea sa.

De asemenea, Autoritatea națională de supraveghere a constatat că societatea comercială, în calitate de operator, nu a informat persoanele vizate cu privire la încălcarea securității datelor lor cu caracter personal, prin divulgarea neautorizată, de către un angajat al său, deși aceste date, divulgate în mod neautorizat, pot conduce la prejudicii fizice, materiale sau morale aduse persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză.

Totodată, Autoritatea națională de supraveghere a constatat că operatorul investigat a stocat informații (module cookies care nu erau necesare din punct de vedere tehnic în funcționarea site-ului) sau a obținut accesul la informația stocată în echipamentul terminal al utilizatorilor site-ului deținut de către societate, fără obținerea acordului utilizatorului în cauză (prin apăsarea butonului de Accept) și fără furnizarea, anterior exprimării acordului, a unor informații clare și complete, potrivit art. 12 – art. 14 din Regulamentul (UE) 2016/679.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 49.418 lei (echivalentul a 10.000 EURO), pentru încălcarea prevederilor art. 32 alin. (4) din Regulamentul (UE) 2016/679.

În același timp, operatorul a fost sancționat cu două avertismente, pentru încălcarea prevederilor art. 34 din Regulamentul (UE) 2016/679 și respectiv pentru încălcarea art. 4 alin. (5) din Legea 506/2004.

4. FIȘĂ DE CAZ – Prelucrarea excesivă a imaginii clienților și angajaților prin intermediul unui sistem de supraveghere video

Autoritatea națională de supraveghere a fost sesizată cu privire la monitorizarea angajaților și clienților unei societăți comerciale, având ca obiect "salon de coafură și alte activități de înfrumusețare", prin intermediul sistemului de supraveghere video instalat în camera unde se efectuează tratamentele corporale/cosmetice.

Ca urmare a investigației efectuate în acest caz, Autoritatea națională de supraveghere a constatat că operatorul investigat a prelucrat în mod excesiv, prin raportare la scopul în care sunt prelucrate (protejare bunuri/echipamente împotriva unor eventuale distrugerii sau sustrageri, siguranța personalului și a clienților) datele cu caracter personal (imaginea) ale clienților și angajaților săi, prin intermediul camerei video instalate în camera de cosmetică (sala de tratamente corporale), datele astfel prelucrate nefiind adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate ("reducerea la minimum a datelor"), operatorul neputând demonstra respectarea principiilor de prelucrare conform art. 5 alin. (2) din Regulamentul (UE) 2016/679.

Autoritatea națională de supraveghere a mai constatat că operatorul investigat nu a prezentat dovezi din care să rezulte faptul că a asigurat o informare clară, completă și corectă a persoanelor vizate ale căror date cu caracter personal (imagini) se prelucreează prin intermediul sistemului de supraveghere video instalat la sediul acesteia, prin comunicarea tuturor informațiilor prevăzute de art. 13 din Regulamentul (UE) 2016/679 și în condițiile de transparență menționate la art. 12 din Regulamentul (UE) 2016/679.

Ca urmare a investigației efectuate în acest caz, Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 7.417,65 lei (echivalentul a 1.500 euro), pentru încălcarea art. 5 alin. (1) lit. a), b) și c) din Regulamentul (UE) 2016/679, prin raportare la condițiile privind legalitatea prelucrării, stabilite de art. 6 din Regulamentul (UE) 2016/679.

În același timp, operatorul a fost sancționat cu amendă în cuantum de 4.945,10 lei (echivalentul a 1.000 euro), pentru încălcarea art. 12 și art. 13 din Regulamentul (UE) 2016/679.

De asemenea, operatorului i s-au aplicat patru măsuri corective, constând în:

- Informarea persoanelor vizate prin comunicarea într-o formă concisă, transparentă, inteligibilă și ușor accesibilă a tuturor informațiilor prevăzute de art. 13 din Regulamentul (UE) 2016/679 și în condițiile de transparență menționate la art. 12 din Regulamentul (UE) 2016/679;

- Eliminarea utilizării camerei de supraveghere video instalată la nivelul camerei de cosmetică, pentru care nu există un temei legal expres de prelucrare a datelor personale ale clienților și angajaților săi conform art. 6 din Regulamentul (UE) 2016/679;

- Asigurarea conformității cu Regulamentul (UE) 2016/679 a operațiunilor de prelucrare a datelor personale, prin implementarea unor măsuri tehnice și organizatorice adecvate și stabilirea unor reguli adecvate legate de gestionarea imaginilor captate de camerele de supraveghere;
- Interzicerea accesului de la distanță prin internet la imagini și înregistrări, precum și accesarea imaginilor și înregistrărilor numai în situația producerii unor incidente care au legătură cu scopul instalării acestor camere de supraveghere.

Ca urmare, operatorul a comunicat că a oprit supravegherea video din camera în care se efectuează tratamentele corporale/cosmetice.

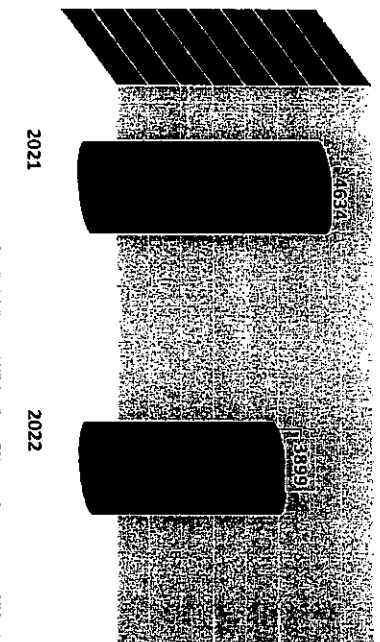
Secțiunea a 3-a: Activitatea de soluționare a plângerilor

1. Prezentare generală

În exercitarea competențelor prevăzute de Regulamentul (UE) 2016/679, de Legea nr.102/2005, și de Legea nr. 190/2018, **Autoritatea națională de supraveghere a primit, pe parcursul anului 2022, un număr total de 3.899 plângeri** care au vizat, în principal, următoarele aspecte:

- condițiile de prelucrare a datelor cu caracter personal, respectiv încălcarea prevederilor art. 5 și 6 din Regulamentul (UE) 2016/679;
- încălcarea drepturilor persoanelor vizate, în special a dreptului de acces al persoanei vizate, de opoziție și a dreptului la ștergerea datelor;
- încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date cu caracter personal.

Plângeri 2021-2022

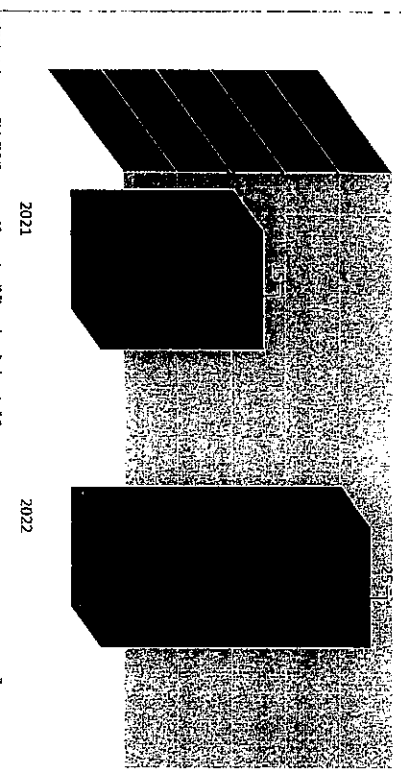


Pentru soluționarea plângerilor considerate admisibile au fost demarate **281** investigații.

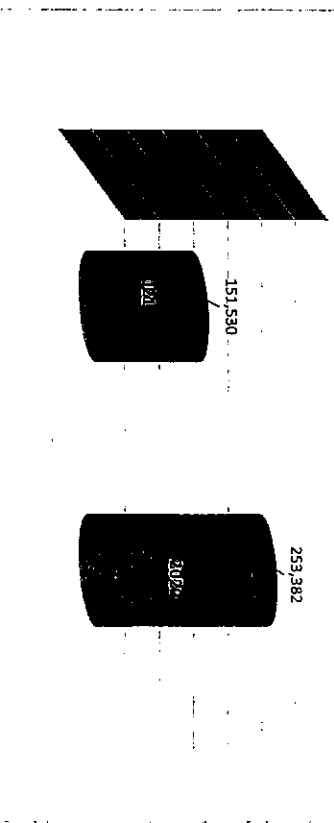
Urmare a investigațiilor efectuate pe baza plângerilor, au fost aplicate următoarele sancțiuni contravenționale:

- > **25 amenzi**, în baza Regulamentului (UE) 2016/679, reprezentând un quantum total de **253.382,28 Lei** (echivalentul a **51.300 EURO**);
- > **90** de avertismente;
- > **60** măsuri corective în baza dispozițiilor art. 58 alin. (2) lit. b) c) și d) din Regulamentul (UE) 2016/679.

Număr amenzi



Valoarea amenzi (lei)

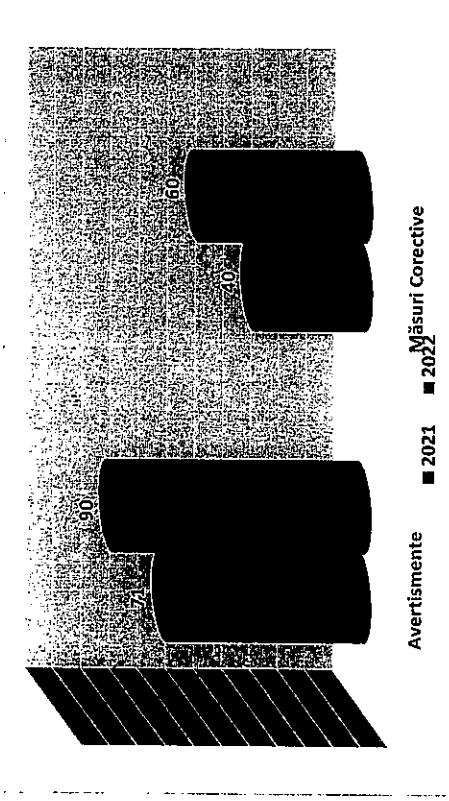


Măsurile corective aplicate de Autoritatea națională de supraveghere au avut ca obiect principal următoarele:

- asigurarea conformității cu Regulamentul (UE) 2016/679 a operațiunilor de colectare și prelucrare ulterioară a datelor personale în cadrul raporturilor juridice existente între operator și persoane vizate;

- transmiterea unui răspuns la cererea petentului, prin comunicarea tuturor informațiilor prevăzute de art. 15 alin. (1) din Regulamentul (UE) 2016/679, adaptate la situația specifică a petentului, prin e-mail și prin poștă, la datele de corespondență indicate de acesta;
- adoptarea procedurilor care să permită gestionarea, analizarea și soluționarea corectă a fiecărei cereri prin care persoanele vizate își exercită drepturile prevăzute de Regulamentul (UE) 2016/679, de o manieră clară și neambiguă, cu respectarea condițiilor prevăzute de art. 12-22 din Regulamentul (UE) 2016/679;

- stabilirea unor perioade limitate de stocare a datelor personale ale persoanelor vizate, cu respectarea art. 5 și 6 din Regulamentul (UE) 2016/679;
- revizuirea și actualizarea măsurilor tehnice și organizatorice implementate, ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, a procedurilor de lucru privind prelucrarea datelor cu caracter personal, precum și implementarea unor măsuri privind instruirea periodică a persoanelor care acționează sub autoritatea operatorului.



2. Principalele constatări rezultate din activitatea de soluționare a plângerilor

A. Încălcarea temeiului legal și a principiilor de prelucrare a datelor personale

În anul 2022, multe dintre investigațiile efectuate și finalizate pentru soluționarea plângerilor adresate Autorității naționale de supraveghere au avut ca obiect verificarea respectării principiilor de prelucrare a datelor cu caracter personal, prevăzute de art. 5 din Regulamentul (UE) 2016/679 și a efectuării prelucrării datelor în conformitate cu condițiile stabilite de art. 6 din același act normativ.

Ca urmare a investigațiilor efectuate, a reieșit că unii operatori nu respectă principiile de prelucrare a datelor, printre cele mai des încălcate fiind cel al "legalității, echității și transparenței", "reducerii la minimum a datelor" și cel al "integrității și confidențialității", reglementate la art. 5 alin. (1) lit. a), c) și f) din Regulamentul (UE) 2016/679.

Totodată, s-a constatat și încălcarea prevederilor art. 5 alin. (2) din Regulamentul (UE) 2016/679, care prevăd că operatorul este responsabil de respectarea acestor principii și trebuie să poată demonstra această respectare (principiul responsabilității).

În ceea ce privește legalitatea prelucrării datelor, reglementată la art. 6 din Regulamentul (UE) 2016/679, a reieșit că operatorii își bazează adesea prelucrările, pe consimțământul persoanelor vizate sau pe interesul legitim urmărit de operator sau de o parte terță, dar fără a avea în vedere toate condițiile care trebuie îndeplinite pentru alegerea acestor temeiuri legale.

De asemenea, accentuăm că, potrivit art. 6 alin. (1) lit. f), ultima teză, din Regulamentul (UE) 2016/679, invocarea unui interes legitim ca temei legal nu se aplică în cazul prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor.

În ceea ce privește calitatea de "parte terță", având în vedere susținerile unor operatori de date în cursul investigațiilor, precizăm că are această calitate orice persoană fizică (alta decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal).

În funcție de caracteristicile fiecărui caz, Autoritatea națională de supraveghere a aplicat sancțiuni contravenționale (avertisment sau amendă) și a dispus măsuri corective pentru remedierea încălcărilor constatate în temeiul art. 58 alin. (2) din Regulamentul (UE) 2016/679.

1. FIȘĂ DE CAZ

O petență a sesizat Autoritatea națională de supraveghere în legătură cu o posibilă încălcare a legislației privind protecția datelor personale de către un operator - instituție de învățământ superior. Astfel, petenta a reclamat că operatorul a dezvăluit datele sale personale (nume și prenume, orașul de domiciliu, codul numeric personal, codul IBAN al contului bancar, numărul de telefon și adresa de e-mail) unor terți, în condițiile în care o cerere a sa adresată acestui operator a fost transmisă în copie către studentul reprezentant de an, care, ulterior, a făcut-o publică prin postarea (fotografică) pe un grup constituit pe rețeaua de socializare whatsapp, folosit de 43 de membri, studenți ai aceluiași an ca petenta.

Petenta s-a adresat operatorului cu privire la aspectele semnalate, dar a fost nemulțumită de răspunsul primit.

În cadrul investigației efectuate în acest caz, s-a constatat că instituția de învățământ superior a dezvăluit în mod ilegal datele personale ale petentei, având în vedere că aspectele invocate în cerere, referitoare la programul de studii, puteau fi diseminate între membrii grupului, fără a face publică identitatea și celelalte date personale ale acesteia.

Astfel, întrucât această cerere cuprindea datele cu caracter personal ale petentei, prin transmiterea copiei cererii unui terț fără anonimizarea datelor, s-a constatat că instituția de învățământ superior a dezvăluit în mod ilegal datele cu caracter personal ale petentei, fără acordul și fără informarea prealabilă a acesteia și cu nesocotirea obligațiilor legale de confidențialitate, încalcând astfel art. 5 alin. (1) lit. a), b), c) și f) și alin. (2) și art. 6 din Regulamentul (UE) 2016/679, deoarece nu a prezentat dovezi că dezvăluirea datelor cu caracter personal ale petentei a fost efectuată cu consimțământul acesteia sau în baza altui temel legal.

Pentru încălcarea acestor prevederi, operatorul a fost sancționat cu avertisment, conform prevederilor Legii nr. 190/2018, care reglementează constatarea contravențiilor și aplicarea sancțiunilor autorităților și organismelor publice.

Totodată, operatorului i s-a stabilit obligatia de a asigura conformitatea operațiunilor de prelucrare a datelor personale ale studenților, astfel încât să se evite divulgarea datelor personale obținute de la aceștia, în afara situațiilor permise de lege.

2. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea unei plângeri în legătură cu divulgarea datelor personale ale unui petent. Astfel, acesta a susținut că adresa pe care a primit-o din partea organelor de poliție a fost postată pe un grup de whatsapp, folosit de avocații dintr-un barou teritorial. Postarea s-a realizat de către unul dintre avocații din cadrul societății civile profesionale de avocați care îl reprezenta pe petent într-un litigiu și căruia petentul îi înaintase această adresă, fără acordul petentului.

În cadrul investigației efectuate în acest caz, motivele invocate de operator pentru a justifica divulgarea, respectiv diseminarea către alți membri ai baroului, nu au putut fi reținute ca legale.

Prin urmare, s-a considerat că divulgarea datelor personale ale petentului în acest context este excesivă și incompatibilă cu scopul inițial pentru care datele au fost colectate, respectiv asistarea și reprezentarea clientului în limitele împuternicirii avocațiale, totodată fiind realizată fără acordul și informarea prealabilă a petentului.

Fără de cele constatate, s-a dispus aplicarea unei amenzi în cuantum de 4.946 lei (echivalentul a 1.000 EURO), pentru încălcarea art. 5 alin. (1) lit. a), b), c) și f) și alin. (2) și a art. 6 din Regulamentul (UE) 2016/679.

Totodată, s-a dispus aplicarea a două măsuri corective vizând, pe de o parte, remedierea aspectelor particulare sesizate de petent (notificarea membrilor grupului de whatsapp în vederea ștergerii adresei), iar pe de altă parte, adoptarea unor măsuri generale privind prelucrarea datelor personale în cadrul raporturilor juridice de asistare și reprezentare a clienților, astfel încât să se evite divulgarea datelor personale obținute de la aceștia, în afara situațiilor permise de lege, inclusiv prin instruirea regulată a persoanelor ce prelucraază date sub autoritatea operatorului.

3. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea unei plângeri în legătură cu dezvăluirea datelor sale personale de către angajatorul unei petente, către unități medicale în cadrul cărora activau medicii semnatari ai certificatelor de concediu medical prezentate de petență în perioada în care era angajată a societății respective. S-a semnalat că această dezvăluire a fost efectuată în scopul investigării realității clinice preținse prin concediile medicale respective. Totodată, petenta a sesizat faptul că, în acest context,



fostul său angajator a transmis o adresă unui alt medic de familie care avea același nume cu medicul de familie la care petenta este înregistrată.

În cadrul investigației efectuate în acest caz, a rezultat că au fost dezvăluite următoarele date personale ale petentei, astfel: adresa de domiciliu, cod numeric personal, funcția deținută, date privind contractul individual de muncă, date privind notificarea de preaviz concediere individuală, date din certificatele de concedii medicale rezultate direct sau indirect, precum concediu pentru îngrijire copil și diagnostice medicale deduse din codurile înscrise pe aceste documente.

Art. 51 din OUG nr. 158/2005 privind concediile și indemnizațiile de asigurări sociale de sănătate prevede, în mod limitativ, entitățile care pot să verifice modul de acordare a concediilor medicale și procedura aplicabilă, competența de control revenind în principal CNAS și caselor de asigurări de sănătate, ce pot fi sesizate de către plătitori. De asemenea, potrivit art. 381 alin. (1) din Legea nr. 95/2006, „în scopul asigurării în orice împrejurare a intereselor pacientului, profesia de medic are la baza exercitării sale independența și libertatea profesională a medicului, precum și dreptul de decizie asupra hotărârilor cu caracter medical”.

Prin urmare, față de prevederile legale citate, solicitările adresate de operator către medicii de familie și unitățile medicale în care activează medicii care au parafat certificatele de concedii medicale emise pe numele petentei nu aveau temei legal și nu se justificau. În plus, au fost dezvăluite în mod ilegal datele petentei către un medic de familie cu care aceasta nu avea niciun fel de raporturi juridice.

Ca atare, art. 9 alin. (2) lit. h) din Regulamentul (UE) 2016/679, invocat de operator nu a putut fi reținut ca un temei legal valid pentru dezvăluirea datelor privind sănătatea în cazul petentei.

De asemenea, interesul legitim invocat de operator nu a putut fi considerat un temei legal pentru prelucrarea datelor privind sănătatea în acest caz, prin raportare la condițiile limitativ prevăzute de art. 9 din Regulamentul (UE) 2016/679, între care nu se regăsește și interesul legitim al operatorului.

În cadrul aceluiași investigații s-a constatat că operatorul, desi a luat la cunoștință de acest incident de la data la care medicul de familie respectiv l-a anunțat în scris că a avut loc o divulgare ilegală de date, nu l-a notificat către Autoritatea Națională de Supraveghere decât după ce a primit o sesizare din partea petentei. Prin urmare, s-a reținut că operatorul nu a



respectat termenul de notificare de cel mult 72 de ore de la data la care a luat cunoștință de încălcarea securității datelor personale.

Față de cele constatate, s-a dispus aplicarea unei amenzi în cuantum de 24.740 lei (echivalentul a 5.000 EURO), pentru încălcarea art. 5 alin. (1) lit. a), c), alin. (2), art. 6 și 9 din Regulamentul (UE) 2016/679, precum și un avertisment pentru nerespectarea termenelor prevăzute de art. 33 din aceleași dispoziții legale.

Totodată, s-a pus în vedere operatorului ca pe viitor să notifice încălcările de securitate a datelor personale cu respectarea termenelor legale și prin folosirea formularului de notificare on-line disponibil pe site-ul www.dataprotection.ro (la secțiunea “Operatori”).

4. FIȘĂ DE CAZ

Un petent a sesizat Autoritatea Națională de Supraveghere că o instituție publică i-a dezvăluit datele cu caracter personal (nume, prenume, adresă, telefon, CNP), prin transmiterea reclamațiilor sale către două societăți de utilitate publică.

În cadrul investigației s-a constatat că operatorul a prelucrat datele cu caracter personal ale petentului, în contextul transmiterii copiilor reclamațiilor sale către două societăți de utilitate publică, fără respectarea principiilor de prelucrare a datelor cu caracter personal: “legalitate, echitate și transparență”, “limitări legate de scop” și “reducerea la minimum a datelor”, precum și a condițiilor de legalitate a prelucrării.

La finalizarea demersurilor întreprinse, Autoritatea Națională de Supraveghere a sancționat operatorul cu avertisment, pentru încălcarea prevederilor art. 5 alin. (1) lit. a, b), c) și alin. (2) din Regulamentul (UE) 2016/679 și prin raportare la dispozițiile art. 6 alin. (1) din Regulamentul (UE) 2016/679.

Totodată, Autoritatea Națională de Supraveghere a dispus operatorului să ia măsuri de revizuire a procedurilor interne și de instruire a personalului propriu, pentru ca, în toate situațiile, datele personale să fie prelucrate în conformitate cu principiile de prelucrare prevăzute la art. 5 din Regulamentul (UE) 2016/679 și în baza unui temei legal stabilit potrivit art. 6 din aceleași act normativ.

B. Nerespectarea drepturilor reglementate de Regulamentul general privind protecția datelor



În anul 2022, nerepectarea drepturilor persoanelor vizate a constituit obiectul multor plângeri adresate Autorității naționale de supraveghere.

Ca urmare a investigațiilor efectuate, s-a constatat faptul că unii operatori nu au soluționat cererile adresate de persoanele vizate (în special cele prin care și-au exercitat dreptul de acces și dreptul de ștergere) sau nu au respectat termenul în care erau obligați, conform prevederilor art. 12 alin. (3) din Regulamentul (UE) 2016/679, să furnizeze persoanelor vizate informații privind acțiunile întreprinse în urma cererilor transmise.

În urma investigațiilor efectuate pentru soluționarea plângerilor, operatorilor li s-a cerut să ia măsurile tehnice și organizatorice necesare, astfel încât să se asigure conformitatea operațiunilor de prelucrare cu dispozițiile Regulamentului (UE) nr. 2016/679, respectiv să fie respectate, în toate cazurile, drepturile persoanelor vizate prevăzute de Regulamentul (UE) 2016/679, inclusiv prin adoptarea unor proceduri interne privind modul de soluționare a cererilor depuse de persoanele vizate în temeiul Regulamentului (UE) nr. 2016/679 (art. 12-22) și comunicarea unor răspunsuri către persoanele vizate în cadrul termenelor legale.

1. FIȘĂ DE CAZ

Un petent a reclamat refuzul unei instituții financiar-bancare de a-i comunica o copie a clauzelor referitoare la protecția datelor personale cu privire la transferul datelor sale personale, aferente contractului de cesiune a creanțelor încheiat de instituția financiar-bancară cu un importator dintr-un stat terț.

Prin răspunsul la cererea sa, instituția financiar-bancară a invocat o serie de clauze de natură confidențială din acest contract, ca motiv pentru a justifica refuzul. Petentul a revenit cu o cerere, insistând asupra faptului că dorește să primească informații legate de prelucrarea datelor personale pe care are dreptul să le solicite, nefiind interesat în primirea clauzelor confidențiale din contractul de cesiune.

În baza art. 13 alin. (1) lit. f) din Regulamentul (UE) 2016/679, operatorul de date este obligat să informeze persoanele vizate cu privire la: "dacă este cazul, intenția operatorului de a transfera date cu caracter personal către o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menționate la articolul 46 sau 47 sau la articolul 49 alineatul (1) al



doilea paragraf, o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție".

Potrivit art. 46 alin. (2) lit. c) din Regulamentul (UE) 2016/679, se consideră a fi garanții adecvate pentru transferul datelor cu caracter personal către o țară terță sau o organizație internațională care nu face obiectul unei decizii a CE privind nivelul adecvat de protecție "clauzele standard de protecție a datelor adoptate de Comisie în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2)".

În ceea ce privește dreptul de acces, art. 15 alin. (2) din Regulamentul (UE) 2016/679, prevede următoarele: "În cazul în care datele cu caracter personal sunt transferate către o țară terță sau o organizație internațională, persoana vizată are dreptul să fie informată cu privire la garanțiile adecvate în temeiul articolului 46 referitoare la transfer."

Având în vedere cadrul legal mai sus prezentat, Autoritatea națională de supraveghere a considerat că subzistă obligația operatorului de a pune la dispoziția persoanelor vizate o copie a clauzelor referitoare la protecția datelor cu caracter personal, din contractul încheiat de acesta cu importatorul de date din țara terță.

În cadrul investigației efectuate în acest caz, a rezultat că operatorul a dat curs cererii petentului ulterior începerii investigației Autorității naționale de supraveghere, transmițându-i în copie contractul privind transferul de date cu caracter personal încheiat între operator, în calitate de cedent/exportator și o societate dintr-un stat terț, în calitate de cesionar/importator, dar cu depășirea termenului de 3 luni prevăzut de art. 12 alin. (3) din Regulamentul (UE) 2016/679 și cu încălcarea prevederilor art. 15 alin. (2) din Regulamentul (UE) 2016/679, prin raportare la prevederile art. 13 alin. (1) lit. f) și art. 46 din Regulamentul (UE) 2016/679.

Față de cele constatate, s-a dispus aplicarea unui avertisment pentru încălcarea art. 12 alin. (3) și art. 15 alin. (2) din Regulamentul (UE) 2016/679.

2. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea plângerii depuse de un petent care a reclamat că a primit pe numărul său de telefon mai multe mesaje comerciale tip SMS, din partea unei societăți comerciale. În urma solicitării petentului de a nu-i mai fi utilizate datele în scop de marketing, deși operatorul l-a informat



că datele sale nu vor mai fi prelucrate în acest scop, acesta a continuat să primească mesaje comerciale nesolicitate, tip SMS, din partea operatorului.

În cadrul investigației, s-a constatat că operatorul a încălcat dreptul de opoziție al petentului, întrucât i-a transmis mesaje comerciale în scop de marketing, deși acesta își exercitase dreptul de opoziție cu privire la utilizarea numărului său de telefon în acest scop.

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 9,883.60 lei (echivalentul a 2.000 EURO), pentru încălcarea art. 21 din Regulamentul (UE) 2016/679.

3. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată de un petent în legătură cu încălcarea dreptului la ștergere a datelor sale cu caracter personal.

Petentul a susținut că a primit un SMS prin care era informat cu privire la ofertele societății, în condițiile în care anterior acesta solicitase ștergerea conținutului său, inclusiv a datelor personale nerelevante.

Societatea îi comunicase petentului faptul că îi confirmă ștergerea conținutului, precizându-i, de asemenea, că "în cazul în care am identificat informații care prin natura lor este necesar să fie păstrate ulterior ștergerii conținutului, aceste informații nu au fost șterse având în vedere legislația aplicabilă sau interesele noastre legitime (cum ar fi, unde este cazul, facturi, certificate de garanție, solicitările primite etc.). Perioada de păstrare a acestor informații este stabilită în funcție de temeiul legal aplicabil, acestea urmând a fi șterse la împlinirea acestor termene. Dorim să vă comunicăm că păstrăm facturile fiscale conform articolului 23 alin. (1) din Legea contabilității nr. 82/1991 și articolului 109 alin. (3) din Legea nr. 207/2015 privind Codul de procedură fiscală și garanțiile asociate produselor achiziționate pe toată perioada de valabilitate a acestora, respectiv 10 ani."

Ca urmare a investigației efectuate, s-a constatat că operatorul nu a adoptat toate măsurile necesare pentru a da curs efectiv cererii petentului de a i se șterge conținutul și datele personale nerelevante, astfel încât a continuat să prelucreză datele acestuia prin trimiterea către numărul său de telefon a unui SMS prin care era informat cu privire la ofertele societății.



Față de cele constatate, operatorul a fost sancționat contravențional cu amendă în cuantum de 4.918,6 lei (echivalentul a 1.000 EURO), pentru încălcarea dispozițiilor art. 17 din Regulamentul (UE) 2016/679.

De asemenea, s-a recomandat operatorului să ia măsuri tehnice și organizatorice astfel încât să se asigure că dă curs efectiv cererilor prin care se exercită drepturile persoanelor vizate prevăzute de Regulamentul (UE) 2016/679, inclusiv dreptul de ștergere prevăzut de art. 17.

4. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată de un petent în legătură cu faptul că i-a fost încălcat dreptul de acces.

Astfel, petentul a reclamat refuzul unei societăți de a-i furniza informații cu privire la categoriile de date cu caracter personal referitoare la persoana sa pe care societatea le deține, în ce scopuri sunt folosite aceste date, perioada de păstrare a datelor, terți cărora le-au fost divulgate datele și temeiul legal al dezvăluirii, dacă datele sale au fost parte într-un proces decizional automat.

Ca urmare a investigației efectuate, Autoritatea națională de supraveghere a constatat că operatorul a încălcat dispozițiile art. 12 și 15 din Regulamentul (UE) 2016/679, întrucât nu a făcut dovada că a transmis un răspuns petentului la cererea acestuia prin care a solicitat informații cu privire la prelucrarea datelor sale cu caracter personal.

Față de aceste constatări, operatorul a fost sancționat contravențional cu avertisment pentru încălcarea dispozițiilor art. 12 și art. 15 din Regulamentul (UE) 2016/679.

De asemenea, au fost aplicate și următoarele măsuri corective:

- adoptarea unor proceduri interne privind modalitatea de soluționare a cererilor depuse de persoanele vizate în temeiul Regulamentului (UE) nr. 2016/679 (art. 12-22), respectarea, în toate cazurile, a dispozițiilor aplicabile privind analiza și soluționarea fără întârziere a acestor cereri și comunicarea unor răspunsuri către persoanele vizate în cadrul termenelor legale, precum și instruirea regulată a personalului operatorului în acest sens;
- transmiterea un răspuns punctual petentului.



5. FIȘĂ DE CAZ

Un petent a sesizat Autoritatea națională de supraveghere în legătură cu o posibilă încălcare a legislației privind protecția datelor personale de către o societate comercială, deoarece la cererile prin care și-a exercitat dreptul de acces la propriile date, respectiv la imaginea sa preluată prin intermediul sistemului de supraveghere instalat în unul dintre magazinele societății, a primit doar o parte dintre aceste date.

Ca urmare a investigației efectuate, a reieșit că operatorul nu a comunicat la cererile petentului toate informațiile solicitate de acesta, respectiv o copie a propriilor sale date (imagini), cu toate că petentul furnizase suficiente detalii pentru a permite identificarea imaginilor cerute: locul supus monitorizării, data înregistrării și intervalul orar, durata acestora, inclusiv elementele necesare pentru identificarea sa prin transmiterea unei copii a actului de identitate (în care puteau fi vizualizate doar numele și prenumele și poza).

În plus, s-a constatat că, la data depunerii cererii de către petent, prin care a solicitat acces la datele sale, acestea erau încă disponibile, neexpirând termenul de stocare a acestora.

Având în vedere prevederile art. 15 din Regulamentul (UE) 2016/679, comunicarea unei înregistrări video ce conține date (imagini) care privesc persoana vizată, ca urmare a exercitării dreptului de acces de către aceasta, reprezintă o obligație a operatorului, comunicarea imaginilor efectuându-se de operator prin luarea măsurilor de obturare ("blurare") a acelor date care ar putea să aducă atingere drepturilor și libertăților altor persoane fizice, dacă este cazul. Prin urmare, operatorul era obligat să adopte o serie de măsuri tehnice și organizatorice, pentru a permite deplina exercitare a dreptului de acces al persoanei vizate, cu respectarea în același timp a drepturilor altor persoane fizice.

În acest context, operatorul de date a fost sancționat cu amendă în cuantum de 98.889,4 lei (echivalentul a 2.000 EURO), pentru încălcarea prevederilor art. 15 alin. (3) din Regulamentul (UE) 2016/679 și i s-a aplicat măsura corectivă de a comunica petentului toate imaginile solicitate de acesta, în măsura în care mai sunt disponibile, cu blurarea imaginilor care duc la identificarea altor persoane.

6. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea plângerii depuse de un petent care a reclamat publicarea pe youtube a unei filmări ce



conținea un extras din înregistrarea unui curs de formare profesională organizat on-line de o societate comercială, curs la care a participat petentul în calitate de persoană fizică, în condițiile în care nu i s-a cerut în prealabil acordul și nici nu a fost informat în legătură cu înregistrarea și, ulterior, cu dezvăluirea acesteia în alte scopuri.

Potentul s-a adresat operatorului cu o cerere prin care și-a exercitat dreptul de acces, însă nu a primit niciun răspuns. În cererea sa în care a invocat art. 15 din Regulamentul (UE) 2016/679, petentul a solicitat comunicarea informațiilor despre datele sale personale prelucrate de către operator, scopul și temeiul prelucrării datelor sale în contextul difuzării în mediul online, destinării către care au fost divulgate datele sale, precum și rezultatul investigației incidentului.

În cadrul investigației efectuate, a rezultat că operatorul a trimis un răspuns petentului doar prin e-mail și numai ulterior începerii investigației Autorității naționale de supraveghere, cu toate că art. 12 alin. (3) din Regulamentul (UE) 2016/679 impune operatorilor obligația de a furniza persoanei vizate informații privind acțiunile întreprinse în urma unei cereri în temeiul articolelor 15-22, fără întârzieri nejustificate și în orice caz în cel mult o lună de la primirea cererii, ori în cel mult trei luni, cu obligația justificării prelungirii termenului în cadrul termenului de o lună, aspecte nedovedite de către operator în acest caz.

De asemenea, s-a constatat că în acest răspuns operatorul a omis să comunice petentului toate informațiile prevăzute de art. 15 alin. (1) din Regulamentul (UE) 2016/679.

Operatorul nu a prezentat dovezi din care să rezulte că a transmis un răspuns complet, în termenul legal și în formatul cerut de persoana vizată.

Conform declarațiilor operatorului, înregistrarea audio-video a sesiunii de formare profesională la care a participat petentul nu a fost înregistrată/realizată de către operator, pe parcursul derulării cursului on line nefiind stocate imagini, filmări sau alte date cu caracter personal în cadrul platformei, însă a fost probabil realizată de către unul dintre participanții la curs cu propriile dispozitive, cu toate că s-a adus la cunoștința acestora interdicția realizării de înregistrări.

Față de cele constatate, s-a dispus aplicarea unui avertisment pentru încălcarea art. 15 alin. (1) și (3) din Regulamentul (UE) 2016/679, coroborat cu art. 12 alin. (3) din Regulamentul (UE) 2016/679.

Totodată, s-a aplicat o măsură corectivă vizând transmiterea unui răspuns la cererea petentului, prin comunicarea tuturor informațiilor prevăzute de art. 15 alin. (1) din



Regulamentul (UE) 2016/679, adaptate la situația sa specifică, prin e-mail și prin poștă, la datele de corespondență indicate de acesta.

C. Încălcarea regulilor de confidențialitate și securitate a prelucrărilor de date cu caracter personal

În cursul anului 2022, Autoritatea națională de supraveghere a efectuat o serie de investigații care au vizat, printre altele, nerespectarea de către operatori a dispozițiilor Regulamentului (UE) nr. 2016/679 sub aspectul măsurilor de securitate și confidențialitate a datelor personale prelucrate.

Astfel, urmare a plângerilor primite și reținute spre investigare, s-a constatat în unele situații că operatorii fie nu au aplicat măsuri tehnice adecvate care să prevină accesul ilegal ori divulgarea neautorizată a datelor personale, fie nu au implementat măsuri organizatorice suficiente, cum ar fi instruirea regulată a persoanelor care prelucrează date sub autoritatea lor sau verificarea respectării instrucțiunilor date.

În astfel de cazuri, s-a dispus sancționarea contravențională a operatorilor și aplicarea în consecință a unor măsuri corective.

1. FIȘĂ DE CAZ

Printr-o petiție transmisă Autorității naționale de supraveghere, o persoană fizică a reclamat că o societate a transmis un mesaj comercial prin poșta electronică către mai multe persoane, dezvăluind astfel adresele de e-mail ale acestora.

În cadrul investigației efectuate în acest caz, s-a constatat că operatorul nu a adoptat suficiente măsuri de securitate pentru a asigura confidențialitatea datelor personale ale persoanelor vizate, conform obligațiilor impuse de art. 32 din Regulamentul (UE) 2016/679, fapt ce a dus la trimiterea unui mesaj către adresele de poștă electronică aparținând unui număr de 810 persoane fără ascunderea acestora, permițând astfel divulgarea neautorizată a adreselor de e-mail către ceilalți destinatari.

În consecință, s-a dispus sancționarea contravențională a operatorului, cu amendă în cuantum de 14,826.90 lei (echivalentul a 3.000 EURO), pentru încălcarea art. 32 din Regulamentul (UE) 2016/679.



Totodată s-a dispus măsura corectivă, de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de prelucrare a datelor personale, prin implementarea unor măsuri tehnice și organizatorice adecvate în cazul transmiterii la distanță a datelor personale, inclusiv sub aspectul instruirii regulate a persoanelor care prelucrează date sub autoritatea sa (angajați sau colaboratori).

2. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea plângerii depuse de un petent care a reclamat divulgarea de către o societate comercială a datelor privind salariile unor angajați, disponibile în calculatorul pe care acesta l-a primit în urma unei operațiuni de casare a obiectelor. În documentele stocate pe acel calculator erau disponibile informații precum: loc de muncă, nume, prenume, funcție, salariu de încadrare, sumă avans, cont bancar, nume, coduri numerice personale).

În cadrul investigației efectuate în acest caz, s-a constatat că acest calculator a fost alocat petentului, fără să fie încheiat un proces-verbal de predare-primire cu acea ocazie. De asemenea, nu a rezultat că, anterior predării echipamentelor către petent, s-ar fi efectuat operațiuni de verificare și ștergere a documentelor din unitatea centrală a calculatorului. În acest fel, petentul a avut acces neautorizat, în afara atribuțiilor sale de serviciu, la date personale ale angajaților sau foștilor angajați ai operatorului. Mai mult decât atât, petentul a putut să acceseze fișiere din unitatea centrală a calculatorului, întrucât nu erau paroliate.

Totodată, nu au fost prezentate dovezi din care să rezulte că operatorul a luat legătura cu petentul pentru a-i solicita să ia măsuri de ștergere, distrugere, după caz, a informațiilor personale la care a avut acces.

Ca atare, s-a reținut că operatorul nu a adoptat suficiente măsuri de securitate, de natură tehnică și organizatorică, pentru a asigura confidențialitatea datelor personale ale angajaților săi/foștilor săi angajați, conform obligațiilor impuse de art. 32 din Regulamentul (UE) 2016/679, fapt ce a dus la accesarea neautorizată a informațiilor privind veniturile salariale ale acestora de către o terță persoană.

Fajă de cele constatate, s-a dispus aplicarea unei amenzi în cuantum de 9.897,4 lei (echivalentul a 2.000 EURO), pentru încălcarea art. 32 alin. (1), (2), (4) din Regulamentul (UE) 2016/679.

De asemenea, s-au aplicat două măsuri corective, pe de o parte, de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operatorilor de prelucrare a datelor personale, prin implementarea unor măsuri tehnice și organizatorice adecvate, inclusiv sub aspectul instruirii persoanelor care prelucrează date sub autoritatea sa, în legătură cu procedura de casare și predare a unor echipamente pe care sunt stocate date personale, dar și sub aspectul restricționării accesului la fișierele ce conțin date personale, precum și al detectării rapide, gestionării și raportării unor situații de încălcare a securității datelor personale (indiferent că ar necesita sau nu notificarea autorității de supraveghere și/sau a persoanelor vizate), iar, pe de altă parte, în scopul contactării petentului pentru a-i solicita să ia măsuri de ștergere, distrugere, după caz, a informațiilor personale la care a avut acces.

3. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată de un petent, în legătură cu faptul că un operator a comunicat petentului, prin poșta electronică, un răspuns adresat altui client, fără ca documentele anexate să fie parolate, așa cum se susținea în conținutul e-mail-ului.

Documentele transmise petentului conțineau următoarele date ale altui client: nume, prenume, adresă, cod client, informații privind reclamația și rezultatele unui control al operatorului de la locul de consum respectiv, informații privind indexul de consum al contorului, date privind facturi și costurile aferente. Petentul a precizat că a trimis o înștiințare către operator privind acest incident.

În cadrul investigației efectuate, a rezultat că mesajul a fost trimis din eroare către petent. Documentele anexate la acest mesaj nu au fost parolate, astfel că toate informațiile aparținând altui client puteau fi vizualizate de către petent.

Operatorul a prezentat dovezi privind trimiterea unui răspuns către petent, nu însă și către persoana lezată ale cărei date personale au fost expuse prin trimiterea eronată a corespondenței. De asemenea, operatorul nu a prezentat dovezi din care să rezulte că a luat măsuri de remediere, în scopul reducerii riscului la care i-au fost supuse datele personale și pentru a preveni pe viitor dezvăluirea sau accesarea ilegală a datelor personale ale acestuia.

În egală măsură, operatorul nu a prezentat dovezi privind notificarea petentului pentru a-i solicita în mod expres ștergerea documentelor primite, care conțineau datele altui

persoane și nici nu a prezentat dovezi privind notificarea acestui incident la Autoritatea națională de supraveghere, încălcând art. 33 din Regulamentul (UE) 2016/679.

Operatorul a mai fost sancționat anterior de Autoritatea națională de supraveghere pentru fapte asemănătoare (trimiterea din eroare a unor documente sau răspunsuri către alte persoane decât clienții în cauză, incidente, de asemenea, notificate de persoanele respective către operator), fără să fi adoptat ulterior suficiente măsuri de securitate care să prevină repetarea unor astfel de incidente, aspecte care au fost luate în considerare la individualizarea sancțiunii aplicate în acest caz.

Față de cele constatate, s-a dispus aplicarea unei amenzi în cuantum de 49.337 lei (echivalentul a 10.000 EURO), pentru încălcarea art. 32 din Regulamentul (UE) 2016/679, precum și a unui avertisment pentru încălcarea art. 33 din Regulamentul (UE) 2016/679.

Totodată, s-au aplicat trei măsuri corective privind:

- punerea în aplicare a unor măsuri de securitate tehnice și organizatorice adecvate specificului prelucrării și riscurilor identificate, pe întreg ciclul de prelucrare a datelor, în special sub aspectul instruirii persoanelor care prelucrează date sub autoritatea operatorului, al verificării regulate a respectării instrucțiunilor transmise acestora, al automatizării anumitor procese prin care să fie reduce riscurile de prelucrare ilegală sau neautorizată a datelor personale, precum și al detectării rapide, gestionării și raportării unor situații de încălcare a securității datelor personale;

- contactarea petentului pentru a-i solicita să ia măsuri de ștergere, distrugere, după caz, a informațiilor personale la care a avut acces în urma primirii corespondenței ce privea alt client al operatorului;

- adoptarea unor măsuri interne de reducere a riscurilor la care au fost expuse datele personale ale clientului său, pentru a preveni pe viitor dezvăluirea sau accesarea ilegală a datelor personale.

D. Prelucrarea datelor cu caracter personal de către autorități publice

Plângerile adresate, în anul 2022, Autorității naționale de supraveghere au vizat și prelucrarea datelor personale de către autorități publice, fiind reclamate aspecte referitoare la dezvăluirea datelor cu caracter personal pe site-urile proprii, modalitatea de soluționare a



cererilor prin care persoanele fizice și-au exercitat drepturile reglementate de Regulamentul (UE) 2016/679.

În vederea soluționării plângerilor considerate admisibile, Autoritatea națională de supraveghere a efectuat o serie de investigații, în urma cărora operatorii au fost sancționați, în principal, pentru nerespectarea principiilor legate de prelucrarea datelor cu caracter personal, a condițiilor de prelucrare a datelor, a drepturilor persoanelor vizate și a securității prelucrării datelor cu caracter personal.

1. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea plângerilor ce vizau publicarea pe internet a datelor personale ale unui petent, fără consimțământul acestuia, date aferente rezultatelor la un concurs organizat de angajatorul său (un spital public) în cadrul unor anunțuri.

Totodată, au fost divulgate către presă anumite informații privind funcția și locul său de muncă.

În cadrul investigației efectuate, s-a constatat că operatorul nu a prezentat dovezi cu privire la temeiul legal, stabilit în conformitate cu dispozițiile art. 5 și 6 din Regulamentul (UE) 2016/679, în baza căruia să fie obligat să publice să publice pe internet nominal datele personale ale petentului. Potrivit răspunsului operatorului, secretarul comisiei de concurs a omis să solicite petentului să își exprime acordul cu privire la afișarea nominală a rezultatelor concursului.

Făță de cele constatate, s-a dispus aplicarea unui avertisment pentru încălcarea art. 5 alin. (1) lit. a), c) și alin. (2), coroborate cu art. 6 din Regulamentul (UE) 2016/679.

De asemenea, prin planul de remediere, s-a pus în vedere operatorului să adopte măsuri conștând în revizuirea procedurilor existente și analizarea tuturor cazurilor de prelucrare efectuate, în vederea identificării corecte a temeiului legal de prelucrare, prin raportare la dispozițiile art. 6 și după caz, art. 9 și 10 din Regulamentul (UE) 2016/679, precum și instruirea corespunzătoare a persoanelor care prelucrează date sub autoritatea operatorului, astfel încât să se evite dezvăluirea ilegală sau neautorizată a datelor personale ale persoanelor vizate, inclusiv în cazul concursurilor organizate de operator.



2. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată de un petent cu privire la încălcarea obligației de a desemna un responsabil cu protecția datelor de către o instituție publică.

Petentul a susținut că a solicitat operatorului informații cu privire la datele de contact ale responsabilului cu protecția datelor, deoarece pe site-ul autorității respective nu au fost identificate informații cu privire la datele de contact ale acestuia, dar reprezentanții instituției nu au dat curs acestei solicitări.

În urma demersurilor efectuate, s-a constatat că autoritatea reclamată nu a prezentat dovezi că a îndeplinit obligația de a desemna un responsabil cu protecția datelor personale, până la data efectuării investigației de către Autoritatea națională de supraveghere, conform art. 37 alin. (1) lit. a) din Regulamentul (UE) 2016/679, raportat la art. 2 alin. (1) lit. a) și art. 10 din Legea nr. 190/2018 și de a comunica datele de contact ale acestuia către public și către Autoritatea națională de supraveghere, potrivit art. 37 alin. (7) din Regulamentul (UE) 2016/679.

Pentru faptele constatate, operatorul a fost sancționat contravențional cu avertisment, pentru încălcarea dispozițiilor art. 37 alin. (7) din Regulamentul (UE) 2016/679, însoțit de o măsură de remediere, respectiv luarea măsurilor necesare astfel încât să se asigure respectarea prevederilor Regulamentul (UE) 2016/679, inclusiv prevederile art. 37 – 39 din Regulamentul (UE) 2016/679 referitoare la responsabilul cu protecția datelor.

3. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată de un petent cu privire la datele ce l-au fost solicitate de către o autoritate a administrației publice, în scopul decontării carburantului utilizat pentru deplasarea interurbană a unei persoane cu handicap, raportat la prevederile art. 24 alin. (9) din Legea nr. 448/2006 privind protecția și promovarea drepturilor persoanelor cu handicap, republicată.

Ca urmare a investigației, s-a constatat că autoritatea publică a prelucreat datele personale ale persoanei care însoțește persoana cu handicap și asigură conducerea autovehiculului în timpul deplasării acestei persoane, fără să existe un temei legal expres, în conformitate cu art. 5 alin. (1) lit. a) și art. 6 din Regulamentul (UE) 2016/679.

Totodată, nu au fost prezentate suficiente argumente cu privire la caracterul necesar al prelucrării datelor cu caracter personal solicitate petentului, cuprinse în copile documentelor solicitate acestuia (ex. carte de identitate a mașinii, permisul de conducere, rovinleta,) pentru scopurile declarate, prin raportare la art. 5 alin. (1) lit. c) din Regulamentul (UE) 2016/679.

În acest context, operatorul de date a fost sancționat pentru că a prelucrat datele personale ale persoanei care a asigurat conducerea autovehiculului în timpul deplasării interurbane a persoanei cu handicap, în mod excesiv și fără să existe un temel legal expres în acest sens, fiind încălcate așadar principiile prevăzute de art. 5 alin. (1) a) și c) din Regulamentul (UE) 2016/679, precum și condițiile de legalitate a prelucrării prevăzute de art. 6 din Regulamentul (UE) 2016/679.

De asemenea, prin planul de remediere, s-a dispus ca operatorul să ia măsuri pentru prelucrarea datelor personale în conformitate cu art. 5 și art. 6 din Regulamentul (UE) 2016/679, în scopul decontării carburantului necesar deplasării cu autoturismul a persoanei cu handicap, conform atribuțiilor legale și în limitele stabilite de actele normative în vigoare.

4. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea plângerilor unui petent, privind transmiterea de către o primărie de municipiu a unui mesaj legat de gestionarea cererilor depuse pentru eliberarea actelor de identitate, fiind vizibile adresele de e-mail ale tuturor destinatarilor. La aceeași dată, petentul a semnalat această problemă operatorului, însă nu a primit niciun răspuns.

În cadrul investigației efectuate în acest caz, s-a constatat că o persoană aflată sub autoritatea operatorului a divulgat din eroare adresele de e-mail ale unor persoane fizice (95 de adrese de e-mail), cu ocazia unei informații trimise prin e-mail. Anterior investigației, nu fusese elaborată o procedură operațională privind comunicarea prin e-mail care să fi prevăzut includerea adreselor de e-mail ale destinatarilor în rubrica "BCC" ("Being carbon copy"), ce nu permite vizualizarea acestora de către celelalte persoane către care este trimisă o corespondență electronică.

Totodată, nu au fost prezentate dovezi ale instruirii persoanelor ce prelucreză date sub autoritatea operatorului, cu privire la aplicarea unor astfel de reguli de păstrare a

confidențialității datelor. De asemenea, nu fuseseră luate măsuri de informare a persoanelor vizate sau de notificare a acestuia incident către Autoritatea națională de supraveghere.

Prin urmare, s-a reținut că operatorul nu a adoptat suficiente măsuri de securitate pentru a asigura confidențialitatea datelor personale ale persoanelor fizice ce beneficiază de serviciile sale (în speță, eliberarea actelor de identitate), conform obligațiilor impuse de art. 32 din Regulamentul (UE) 2016/679.

Față de cele constatate, s-a dispus aplicarea unui avertisment, pentru încălcarea art. 32 din Regulamentul (UE) 2016/679.

Prin planul de remediere stabilit s-a pus în vedere operatorului să implementeze măsuri tehnice și organizatorice adecvate în cazul transmiterii la distanță a datelor personale, care să urmărească inclusiv asigurarea confidențialității datelor personale prelucrate, instruirea regulată a persoanelor care prelucreză date sub autoritatea operatorului, detectarea rapidă, gestionarea și raportarea unor situații de încălcare a securității datelor personale (indiferent că ar necesita sau nu notificarea autorității de supraveghere și/sau a persoanelor vizate) și să contacteze, totodată, pe e-mail toate persoanele cărora li s-a trimis mesajul din eroare, pentru a le solicita să ia măsuri de neutilizare, ștergere, distrugere, după caz, a informațiilor personale la care au avut acces.

E. Prelucrare date proprietari/locatari de către asociații de proprietari

Printre aspectele reclamate de petenți în anul 2022, s-au numărat cele care referitoare la prelucrarea datelor cu caracter personal de către asociațiile de proprietari.

În acest context, Autoritatea națională de supraveghere a fost sesizată, în principal, cu privire la instalarea nelegală a camerelor de supraveghere video, în special pe paliere, cu privire la afișarea la avizierul condominiului a unor documente care conțineau date cu caracter personal ale proprietarilor, precum și referitoare la nerespectarea drepturilor persoanelor vizate.

1. FIȘĂ DE CAZ

Un petent a transmis Autorității naționale de supraveghere mai multe plângeri prin care a reclamat o asociație de proprietari pentru încălcarea dreptului de acces. Aspectele reclamate au vizat refuzul operatorului de a-i furniza o copie a unei înregistrări audio/video,

captate prin intermediul camerei care supraveghează casieria blocului și lipsa răspunsurilor la cererile petentului de exercitare a dreptului de acces la date.

În urma investigației efectuate, s-a constatat că asociația de proprietari a încălcat prevederile art. 12 și 15 din Regulamentul (UE) 2016/679, întrucât nu a comunicat o copie a înregistrărilor video care îl privesc pe petent, captate prin camera de supraveghere video care surprinde casieria asociației și nu a transmis informații complete la cererile petentului de exercitare a dreptului de acces.

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat operatorul cu avertisment, pentru încălcarea prevederilor art. 12 și 15 din Regulamentul (UE) 2016/679.

2. FIȘĂ DE CAZ

Un petent a sesizat Autoritatea națională de supraveghere cu privire la faptul că asociația de proprietari i-a dezvăluit datele cu caracter personal (nume, prenume, domiciliu, CNP, informații dintr-un dosar civil), cuprinse în cererea sa de chemare în judecată îndreptată împotriva asociației, către o societate care realizează activități de administrație pentru operatorul reclamat și care le-a transmis ulterior către toți membrii asociației de proprietari, prin intermediul poștei electronice.

În cadrul investigației s-a constatat că operațiunea de transmitere a cererii de chemare în judecată a petentului, cuprinzând datele cu caracter personal ale acestuia (nume, prenume, domiciliu, reședință, CNP, informații dintr-un dosar civil în care societatea care realizează activități de administrare nu are nicio calitate), de asociația de proprietari către societatea care realizează activități de administrație, nu este reglementată, cel puțin sub aspectul obiectului, naturii și categoriilor de date cu caracter personal, de documentul transmis de asociația de proprietari Autorității naționale de supraveghere ca urmare a solicitării de a comunica "contractul sau actul juridic încheiat între asociația de proprietari și societatea care realizează activități de administrație, raportat la prevederile art. 28 alin. (3) din Regulamentul (UE) 2016/679".

Totodată, s-a constatat că transmiterea, prin poșta electronică, către membrii asociației de proprietari a cererii de chemare în judecată a petentului, cuprinzând datele cu caracter personal ale acestuia (nume, prenume, domiciliu, reședință, CNP, informații dintr-

un dosar civil), îndreptată împotriva asociației de proprietari, nu s-a realizat cu respectarea principiului de prelucrare privind "reducerea la minimum a datelor", scopul declarat de operator, respectiv informarea membrilor asociației de proprietari cu privire la acțiunea introdusă în instanță de către petent, putându-se realiza cu anonimizarea informațiilor legate de codul numeric personal al petentului și domiciliul acestuia (diferit de reședința sa).

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a aplicat operatorului două avertismente, pentru încălcarea prevederilor art. 28 alin. (3) din Regulamentul (UE) 2016/679 și ale art. 5 alin. (1) lit. a), c) și alin. (2), coroborate cu art. 6 din Regulamentul (UE) 2016/679.

F. Prelucrarea datelor cu caracter personal ale angajaților

În cursul anului 2022, Autoritatea națională de supraveghere a primit plângeri prin care petenții au reclamat prelucrarea datelor personale de către angajatori, atât persoane juridice de drept public, cât și de drept privat.

Plângerile au avut ca obiect, în principal, dezvăluirea datelor cu caracter personal ale angajaților fie pe rețeaua de intranet a angajatorului, fie pe pagina oficială de Facebook a acestuia, fie pe un cont creat pe rețeaua whatsapp de către acesta.

Un alt aspect cu care angajații ne-au sesizat în mod frecvent a constat în prelucrarea imaginilor angajaților, prin intermediul camerelor de supraveghere video instalate în birourile sau alte încăperi în care aceștia își desfășoară activitatea.

Ca urmare a investigațiilor efectuate, a reieșit că mulți angajatori, persoane juridice de drept privat, nu au luat măsurile necesare pentru a îndeplini obligațiile stipulate în sarcina lor prin dispozițiile art. 5 din Legea nr. 190/2018, când prelucrează datele angajaților la locul de muncă, prin utilizarea sistemelor de monitorizare prin mijloace de comunicații electronice și/sau prin mijloace de supraveghere video, în scopul realizării intereselor legitime urmărite de operator.

Întrucât sistemele de monitorizare prin mijloace de comunicații electronice și/sau prin mijloace de supraveghere video comportă anumite riscuri în privința drepturilor și libertăților angajaților, înainte de instalarea unor astfel de sisteme de supraveghere, angajatorul trebuie să facă în prealabil o evaluare a riscurilor la care se supune activitatea sa, pentru a stabili necesitatea implementării lor.

Respectarea acestor condiții trebuie să se regăsească la angajații întru-o documentație argumentată temeinic, din care să rezulte prevalența interesului legitim asupra intereselor sau drepturilor și libertăților angajaților, dacă operatorul invocă acest temei de prelucrare.

1. FIȘĂ DE CAZ

În anul 2022 a fost finalizată investigația pentru soluționarea plângerilor prin care un petent a reclamat instalarea unor camere de supraveghere video în birourile din cadrul primăriei unei comune, unde era angajat, precum și postarea pe pagina de facebook a acestei primării a unei fotografii ce conține și imaginea sa, fără consimțământul acestuia.

Petentul a cerut în scris ștergerea postărilor de pe pagina de facebook a primăriei, precum și demontarea camerei video din biroul unde își desfășura activitatea.

De asemenea, un sindicat a cerut dezinstalarea și îndepărtarea tuturor camerelor de supraveghere video instalate în birourile din sediul primăriei, arătându-se că este încălcat dreptul la viața privată a salariaților, prin crearea sentimentului unei "supravegheri continue, o stare de presiune la locul de muncă și disconfort prin monitorizarea permanentă". La această din urmă solicitare, primăria a răspuns precizând că "la instalare, camerele de supraveghere au primit avizul organelor competente".

În cadrul investigației efectuate în acest caz, s-a constatat că la nivelul primăriei respective erau instalate 16 camere de supraveghere video, dintre care 5 erau montate în 4 birouri, printre care și biroul unde își desfășura activitatea și petentul. Pentru instalarea tuturor camerelor de supraveghere video a fost declarat ca scop "asigurarea unei bune monitorizări și a pazei în instituție", iar în birouri, s-a precizat că "activitatea cu publicul este una intensă, astfel încât era necesară o bună supraveghere, atât a personalului, cât și a cetățenilor comunei, în relația cu autoritățile".

Din documentele puse la dispoziție de operator în cadrul investigației, a rezultat că nu erau instalate camere de supraveghere în toate birourile. În consecință, nu au fost prezentate dovezi cu privire la existența unui temei legal, conform art. 6 din Regulamentul (UE) 2016/679, care să permită autorității publice locale utilizarea mijloacelor de supraveghere video în interiorul birourilor și implicit prelucrarea în acest mod a datelor personale ale persoanelor care își desfășoară activitatea în aceste spații.

De asemenea, nu au fost prezentate dovezi cu privire la asigurarea unei informări complete a persoanelor vizate, prin furnizarea tuturor informațiilor prevăzute de art. 13 din

Regulamentul (UE) 2016/679 și cu respectarea condițiilor de transparență de la art. 12 din Regulamentul (UE) 2016/679, dar nici cu privire la adoptarea unor măsuri de securitate adecvate specificului prelucrării, conform art. 32 din Regulamentul (UE) 2016/679.

În ceea ce privește postarea imaginilor cu petentul pe pagina oficială de facebook a primăriei, operatorul a opinat că aceasta "a avut loc ca replică a unei postări a (petentului) pe rețelele de socializare, prin intermediul unei pagini administrate de acesta cu privire la realizarea acestei investiții în cadrul instituției (sala de protocol), postare care aducea atingere instituției, insinuând că "au fost cheltuiți bani publici pentru acoliții primarului", astfel demonstrând că sala are utilitate pentru toți angajații". Un astfel de motiv nu poate fi considerat ca legitimând o dezvălire a imaginii petentului pe pagina oficială de facebook a primăriei, fără consimțământul acestuia, fiind deci contrară principiilor de prelucrare reglementate de art. 5 alin. (1) lit. a), b), c), alin. (2) și condițiilor de legalitate prevăzute de art. 6 din Regulamentul (UE) 2016/679.

Operatorul nu a făcut dovada că a răspuns la cererea petentului și că a luat măsuri pentru ștergerea imaginii sale de pe pagina de facebook a primăriei și pentru demontarea camerei video din biroul unde acesta își desfășura activitatea, încălcând astfel dispozițiile art. 12 alin. (3) raportat la prevederile art. 17 și 21 din Regulamentul (UE) 2016/679.

Cu ocazia investigației, s-a mai constatat că nu era desemnat un responsabil cu protecția datelor, operatorul motivând că instituția are un număr mic de angajați care au delegate și alte atribuții.

Fără de cele constatate, s-a dispus aplicarea a șase sancțiuni contravenționale (avertisment) pentru încălcarea art. 5 alin. (1) lit. a) și (2) și art. 6 din Regulamentul (UE) 2016/679, art. 12 și 13 din Regulamentul (UE) 2016/679, art. 32 alin. (1), (2), (4) din Regulamentul (UE) 2016/679, art. 5 alin. (1) lit. a), b), c), alin. (2) și art. 6 din Regulamentul (UE) 2016/679, art. 12 alin. (3) raportat la prevederile art. 17 și 21 din Regulamentul (UE) 2016/679, art. 37 alin. (1) lit. a) și (7) din Regulamentul (UE) 2016/679, raportat la art. 2 alin. (1) lit. a) și art. 10 din Legea nr. 190/2018.

De asemenea, prin planul de remediere, s-au pus în vedere operatorului următoarele măsuri:

- eliminarea folosirii sistemului de supraveghere video instalat la nivelul birourilor din cadrul primăriei pentru care nu există un temei legal expres de prelucrare a datelor personale ale angajaților săi conform art. 6 din Regulamentul (UE) 2016/679;

- realizarea informării complete a tuturor persoanelor vizate, în legătură cu toate activitățile ce implică prelucrări de date personale, prin furnizarea tuturor informațiilor prevăzute de art. 13 și 14 din Regulamentul (UE) 2016/679, după caz, și cu respectarea condițiilor prevăzute de art. 12 din Regulamentul (UE) 2016/679, atât în scris, cât și pe site/facebook și la sediul primăriei;
- implementarea măsurilor de securitate tehnice și organizatorice adecvate pentru toate prelucrările de date personale, precum și instruirea corespunzătoare a persoanelor care prelucrează date sub autoritatea operatorului, în conformitate cu art. 24, 29 și 32 din Regulamentul (UE) 2016/679;
- respectarea cererii depuse de petent cu privire la ștergerea imaginilor sale de pe pagina oficială de facebook a primăriei, ce făceau obiectul procesului-verbal;
- comunicarea unui răspuns scris la cererea petentului;
- desemnarea unui responsabil cu protecția datelor personale cu respectarea tuturor condițiilor prevăzute de art. 37-39 din Regulamentul (UE) 2016/679 și comunicarea datelor de contact ale acestuia către Autoritatea națională de supraveghere și către public.

2. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată de o petentă cu privire la utilizarea datelor sale cu caracter personal de către propriul angajator, fără consimțământul său, în vederea înscrierii și programării sale pe platforma națională de vaccinare pentru efectuarea vaccinului împotriva Covid-19.

În urma investigației realizate, s-a constatat că angajatorul a utilizat datele cu caracter personal ale petentei (nume, prenume, CNP, serie și număr act de identitate, localitate, județ, adresă de e-mail) în scopul înscrierii și programării acesteia pe platforma națională de programare pentru vaccinarea împotriva Covid-19, fără a face dovada existenței consimțământului petentei și fără existența unei alte situații în care consimțământul nu este necesar.

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 4,945.40 lei (echivalentul a 1.000 EURO), pentru încălcarea prevederilor art. 5 alin. (1) lit. a) și alin. (2) și ale art. 6 din Regulamentul (UE) 2016/679.

3. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea plângerii unui petent care sesizată că angajatorul său, o autoritate publică, a instalat, atât în cadrul autorității, cât și în cadrul birourilor teritoriale subordonate acesteia, un sistem de supraveghere video, iar camerele de supraveghere sunt montate inclusiv în birouri și sunt folosite pentru monitorizarea angajaților.

Ca urmare a investigației efectuate, a reieșit că operatorul trebuia să ia măsuri pentru a se asigura evitarea oricărei utilizări necorespunzătoare a datelor, în scopuri incompatibile cu scopul declarat ("prevenirea efracției, detecției și semnalizării pătrunderii neautorizate, restricționării accesului, supravegherii video și înregistrării imaginilor din zonele de interes sau transmiterii semnalelor către dispeceratele de monitorizare").

Astfel, s-a constatat că datele personale erau utilizate în următoarele scopuri incompatibile: verificarea respectării deciziilor emise de conducătorul instituției, monitorizarea performanței angajaților, respectării programului de lucru sau verificării prezenței angajaților la sediu, ceea ce constituia o încălcare a prevederilor art. 5 alin. (1) lit.(b) din Regulamentul (UE) 2016/679 - limitări legate de scop.

De asemenea, având în vedere scopul declarat al instalării sistemului de supraveghere video, a rezultat că datele angajaților au fost prelucrate excesiv față de scopul declarat.

Astfel, au fost comparate numărul de camerele de supraveghere video montate în interiorul și exteriorul clădirii unde funcționează autoritatea respectivă (27 în interior, dintre care aprox. 15 în birouri, față de doar 5 camere în exterior). Mai mult, a reieșit că la nivelul acestei autorități au fost adoptate și alte măsuri, mai puțin invazive pentru persoanele vizate, pentru realizarea scopului declarat, precum sistemul de alarmare la efracție, control acces.

De asemenea, s-a constatat că nu au fost prezentate dovezi cu privire la existența unui temei legal, conform art. 6 din Regulamentul (UE) 2016/679, care să permită operatorului utilizarea mijloacelor de supraveghere video în interiorul birourilor și, implicit, prelucrarea în acest mod a datelor personale ale persoanelor care își desfășoară activitatea în aceste spații.

Ca urmare, s-a constatat că operatorul a prelucrat ilegal datele personale ale angajaților săi prin intermediul camerelor de supraveghere video instalate atât în unele

să fie indicat un temel legal expres, în scopuri incompatibile cu scopul declarat și fără a fi limitate la ceea ce este necesar în raport cu scopul prelucrării, încalcând astfel art. 5 alin. (1) lit. a), b) și c) și alin. (2) și art. 6 din Regulamentul (UE) 2016/679.

Pentru încălcarea acestor prevederi operatorul a fost sancționat cu avertisment, conform prevederilor Legii nr. 190/2018.

Totodată, prin planul de remediere, s-a dispus ca operatorul să ia măsuri pentru eliminarea folosirii sistemului de supraveghere video instalat în birouri, pentru care nu există un temel legal expres de prelucrare a datelor personale ale angajaților săi.

De asemenea, s-a dispus să nu fie utilizate datele cu caracter personal ale angajaților în scopuri incompatibile cu scopul declarat.

G. Prelucrare date cu caracter personal de către persoane împuternicite

Regulamentul (UE) 2016/679 definește persoana împuternicită de operator ca fiind persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

Totodată, același act normativ stabilește că prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate și obligațiile și drepturile operatorului. Respectivul contract sau act juridic prevede și faptul că persoană împuternicită de operator prelucrează datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului.

O serie de investigații inițiate anterior de Autoritatea națională de supraveghere au fost finalizate în cursul anului 2022, prin sancționarea persoanelor împuternicite de operator pentru prelucrarea datelor cu caracter personal ale persoanelor vizate fără respectarea prevederilor din Regulamentul (UE) 2016/679, în special a dispozițiilor art. 32, care reglementează securitatea prelucrării datelor cu caracter personal.

1. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea plângerii unui petent, referitoare la publicarea pe facebook a unor imagini în care este surprins și acesta. Imaginile proveneau din sistemul de supraveghere video instalat într-o stație de distribuție produse petroliere, fiind filmate de pe monitorul din această stație.

În cadrul investigațiilor efectuate atât la nivelul operatorului, cât și al persoanei împuternicite care administrează stația respectivă, a rezultat că operatorul a adoptat măsuri de securitate și a efectuat instruire repetată, inclusiv în privința condițiilor de utilizare a sistemelor de supraveghere video instalate în stațiile sale, cât și a celor ce vizează permiterea accesului la înregistrări, inclusiv în cazul reprezentantului persoanei împuternicite, care administrează stația de petrol în cauză.

Cu ocazia investigației efectuate în acest caz, persoana împuternicită de operator nu a prezentat dovezi din care să rezulte că, anterior incidentului, angajații săi ar fi participat la cursuri sau sesiuni de instruire prin care să le fie prezentate periodic și în mod specific obligațiile ce le revin, în legătură cu prelucrarea datelor personale prin intermediul sistemului de supraveghere video din cadrul stației, a modului în care trebuie să gestioneze eventuale cereri de acces de către persoanele vizate sau terți a înregistrărilor stocate pe DVR ori a procedurii de notificare a unor incidente de securitate.

De asemenea, nu au fost prezentate dovezi că persoana împuternicită a pus la dispoziție angajaților săi toate informațiile și materialele de instruire realizate de operator, în cadrul sesiunilor de instruire la care a participat coordonatorul stației.

Ca atare, întrucât persoana împuternicită nu a prezentat dovezi din care să rezulte că a adoptat suficiente măsuri tehnice și organizatorice adecvate în vederea asigurării confidențialității datelor personale prelucrate în această calitate, cu privire la imaginile înregistrate prin intermediul sistemului de televiziune instalat în stațiile folosite ca agent, în special sub aspectul instruirii angajaților săi, fapt care a condus la vizualizarea și filmarea de către terțe persoane neautorizate a înregistrărilor preluate de camerele video din punctul său de lucru, imagini care îi priveau pe petent ce au fost ulterior dezvăluite pe o rețea de socializare, s-a reținut în sarcina sa încălcarea art. 29 și art. 32 alin. (4) din Regulamentul (UE) 2016/679.

Fără de cele constatate, s-a dispus aplicarea unei amenzi în cuantum de 4.941,3 lei (echivalentul a 1.000 EURO) și, totodată, a unei măsuri corective astfel încât să fie asigurată



conformitatea operațiunilor de prelucrare a datelor personale cu Regulamentul (UE) 2016/679, prin implementarea unor măsuri tehnice și organizatorice adecvate, în special sub aspectul instruirii persoanelor care prelucrează date sub autoritatea persoanei împuternicite (angajați sau colaboratori), prin organizarea regulată a unor sesiuni de instruire cu acestea, în legătură cu obligațiile ce le revin privind prelucrarea datelor personale prin intermediul sistemului de televiziune instalat în stațiile de petrol, al verificării accesului la înregistrările imaginilor stocate pe DVR, precum și al detectării rapide, gestionării și raportării unor situații de încălcare a securității datelor personale, în relația cu operatorul.

Autoritatea națională de supraveghere a adus aceste măsuri de sancționare și la cunoștința operatorului, căruia i-a recomandat să urmărească respectarea de către persoana împuternicită a măsurii corective, precum și de către celelalte persoane împuternicite care prelucrează date personale în numele și pe seama operatorului.

2. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că o societate comercială a transmis către mai multe persoane, utilizând adrese de poștă electronică la vedere, un mesaj comercial având ca obiect promovarea unui produs.

În urma investigației demarate la operator a rezultat că acesta a derulat o campanie pentru un nou produs, folosind o agenție de marketing, în calitate de împuternicit. Potrivit contractului încheiat cu operatorul, împuternicitului i-a revenit responsabilitatea de a dezvolta site-ul utilizat pentru campania de marketing realizată în numele operatorului, precum și de a asigura gestionarea campaniei (aspectul și managementul bazelor de date, inclusiv gestionarea adresei de e-mail de contact).

Autoritatea națională de supraveghere a realizat o investigație și la persoana împuternicită, constatând că, în cadrul campaniei realizate pentru operator, persoana împuternicită a transmis prin e-mail un mesaj către 27 de persoane.

Din cauza unei erori umane (un parametru al codului de program de trimitere e-mail nu a fost resetat), la fiecare trimitere s-au păstrat și adresele la care s-a trimis anterior în cadrul aceleiași liste de e-mail (27 adrese de e-mail). Astfel, s-au transmis e-mail-uri către 26 de persoane (inclusiv către petent) ce conțineau în câmpul destinatatar și adresele de e-mail ale destinatariilor anteriori.



Ca atare, s-a constatat că persoana împuternicită nu a adoptat suficiente măsuri tehnice și organizatorice în vederea asigurării confidențialității datelor personale prelucrate în calitate de persoană împuternicită a operatorului, conform obligațiilor impuse de art. 32 din Regulamentul (UE) 2016/679, fapt ce a condus la trimiterea unui mesaj comercial către adresele de poștă electronică aparținând unui număr de 26 de persoane, fără blurarea acestora, permițând astfel divulgarea neautorizată a adreselor de e-mail către ceilalți destinatari.

Pentru faptele constatate, persoana împuternicită a fost sancționată cu amendă în cuantum de 4,942.30 lei (echivalentul a 1.000 EURO), pentru încălcarea prevederilor art. 32 alin. (1) lit. b) din Regulamentul (UE) 2016/679, care prevede obligația de a implementa măsuri tehnice și organizatorice adecvate, incluzând capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare.

3. FIȘĂ DE CAZ

Un petent a sesizat Autoritatea națională de supraveghere cu privire la faptul că primește pe numărul său de telefon mobil, din partea unei companii de servicii financiare a cărei activitate principală o constituie transferul de bani, mesaje text tip SMS, referitoare la transferul unor sume de bani către anumite persoane, transmișii pe care petentul susține că nu le-ar fi realizat.

În urma investigației realizate în acest caz, operatorul a comunicat Autorității naționale de supraveghere faptul că prelucrarea numărului de telefon al petentului este rezultatul acțiunilor neautorizate întreprinse de un angajat al persoanei împuternicite (instituție financiar-bancară), la inițierea transferului de bani, prin încălcarea obligațiilor prevăzute în acordul dintre operator și împuternicit.

Astfel, a rezultat că mesajele tip SMS transmise către numărul de telefon al petentului (care cuprindeau datele destinatariilor sumelor de bani) au fost, în fapt, destinate clienților care au folosit serviciile operatorului, pentru a transmite bani, petentul primind aceste SMS-uri ca urmare a introducerii abuzive a numărului său de telefon în câmpul destinatatar numărului de telefon al clienților care au folosit în mod real serviciile operatorului.

Totodată, în cadrul investigației realizate la persoana împuternicită, a rezultat că petentul nu a fost client al persoanei împuternicite (instituție financiar-bancară), nu a solicitat

inițierea unor tranzacții prin intermediul operatorului, iar datele sale personale nu erau asociate cu numărul de telefon, în cadrul informațiilor aferente expeditorului unei tranzacții.

Astfel, în urma investigației efectuate, persoana împuternicită (Instituția financiar-bancară) a fost sancționată cu avertisment, pentru încălcarea art. 5 alin. (1) lit. a) și b) și art. 6 din Regulamentul (UE) 2016/679, întrucât s-a introdus în mod abuziv numărul de telefon aparținând petentului, în cadrul aplicației puse la dispoziție de către operator. Prin această aplicație se inițiau tranzacții în numele operatorului, la solicitarea persoanelor- clienți ocazionali, numărul de telefon fiind utilizat în cadrul a 44 de tranzacții în care petentul nu a fost parte.

Totodată, persoana împuternicită a fost sancționată cu amendă în cuantum de 9,763.60 lei (echivalentul a 2.000 EURO), întrucât a prelucrat date inexacte (numărul de telefon) cu privire la persoane (clienți ocazionali) care au realizat tranzacții de bani prin aplicația operatorului, fiind utilizat numărul de telefon al petentului, fără ca acesta să fie expeditorul tranzacțiilor respective, încălcându-se prevederile art. 5 alin. (1) lit. d) din Regulamentul (UE) 2016/679.

CAPITOLUL IV

ACTIVITĂȚI ÎN DOMENIUL RELAȚIILOR INTERNAȚIONALE

Activitatea Autorității naționale de supraveghere la nivel internațional a fost influențată și în anul 2022 de pandemia COVID-19. Prin urmare, reuniunile externe au fost organizate atât în format fizic, cât și în format videoconferință. Autoritatea națională de supraveghere participând la următoarele grupuri de lucru la nivel european, conferințe, seminarii și alte reuniuni ale organismelor Uniunii Europene sau ale Consiliului Europei în domeniul protecției datelor cu caracter personal, fiind implicată, de asemenea, în activitatea desfășurată în cadrul acestora. Reuniunile includ:

- Comitetul european pentru protecția datelor, respectiv subgrupurile de lucru: BITLE, Cooperare, Calcul amenzii, eGuvernare, Enforcement, Probleme financiare, IT users, Aspecte cheie, Social Media, Tehnologie, Transferuri Internaționale,
- Comitetul Consultativ al Convenției 108 al Consiliului Europei,
- Grupul de coordonare comună în domeniul Schengen,
- Grupul de coordonare comună în domeniul Vizelor.

Comitetul european pentru protecția datelor

În anul 2022, Comitetul european pentru protecția datelor a adoptat **23** avize pe marginea proiectelor de decizii ale autorităților de supraveghere referitoare la regulile corporatiste obligatorii pentru operator/persoane împuternicite de operatori, **3** avize pe marginea proiectului de cerințe de acreditare a unui organism de monitorizare a unui cod de conduită, în conformitate cu art. 41 din Regulamentul (UE) 2016/679, **3** avize pe marginea proiectului de cerințe cu privire la aprobarea cerințelor de acreditare a unui organism de certificare în conformitate cu art. 43 alin. (3) din Regulamentul (UE) 2016/679, **3** avize pe marginea proiectelor de mecanisme de certificare, în conformitate cu art. 42 din Regulamentul (UE) 2016/679, **5** decizii obligatorii în temeiul art. 65 din Regulamentul (UE) 2016/679.



În același timp, Comitetul european pentru protecția datelor a adoptat și emis o serie de orientări cu privire la aplicarea Regulamentului (UE) nr. 2016/679, recomandări, declarații, note de informare, dintre care evidențiem:

➤ Orientările 2/2022 privind aplicarea articolului 60 din Regulamentul (UE) 2016/679 – aceste Orientări, adoptate la 14 martie 2022, se bazează pe cerințele art. 60 din Regulamentul (UE) 2016/679 și clarifică, pentru fiecare alineat în parte, condițiile care decurg din Regulament și din punerea sa în aplicare, scopul fiind de a analiza și de a oferi orientări cu privire la aplicarea concretă a dispozițiilor. Astfel, Orientările tratează interacțiunile dintre autoritățile de supraveghere, pe de o parte, și CEPD și părțile terțe, pe de altă parte, în temeiul art. 60 din Regulamentul (UE) 2016/679. Întrucât procedura de cooperare se referă la activitățile de prelucrare, rezultatul acesteia se referă, prin definiție, la actorii implicați în această prelucrare (persoana vizată, operatorul, persoana/persoanele împuternicite/împuternicite de operator etc.). Cu toate acestea, întrucât obligația de cooperare prevăzută la art. 60 din Regulamentul (UE) 2016/679 se aplică autorităților de supraveghere, documentul se axează pe obligațiile autorității de supraveghere principale și ale altor autorități de supraveghere vizate.

➤ Orientările 4/2021 privind codurile de conduită ca instrumente pentru transferuri – aceste Orientări completează Orientările nr. 1/2019 ale CEPD privind codurile de conduită și organismele de monitorizare prevăzute în Regulamentul (UE) 2016/679 și oferă clarificări cu privire la rolul diferiților actori implicați în stabilirea unui cod care să fie utilizat ca instrument pentru transferuri și prezintă procesul de adoptare cu ajutorul unor diagrame. Scopul prezentelor Orientări este de a specifica aplicarea art. 40 alin. (3) din Regulamentul (UE) 2016/679, referitor la codurile de conduită ca garanții adecvate pentru transferurile de date cu caracter personal către țări terțe, în conformitate cu art. 46 alin. (2) litera (e) din Regulamentul (UE) 2016/679. Acestea urmăresc, de asemenea, să ofere îndrumări practice, inclusiv cu privire la conținutul unor astfel de coduri de conduită, la procesul de adoptare a acestora și la actorii implicați, precum și la cerințele care trebuie îndeplinite și la garanțiile care trebuie furnizate de un cod de conduită pentru transferuri. Orientările ar trebui să constituie, de asemenea, o referință clară pentru toate autoritățile de supraveghere și pentru CEPD și să asiste Comisia Europeană la evaluarea codurilor în mod consecvent și să eficientizeze procedurile implicate în procesul de evaluare.



➤ Orientările 6/2022 privind implementarea practică a reglementărilor pe cale amiabilă – documentul abordează punerea efectivă în aplicare a soluțiilor pe cale amiabilă numai în cazurile care au fost inițiate sub formă de plângere din partea unei persoane vizate, întrucât posibilitatea unei soluționări presupune existența unui litigiu între două entități, în acest caz plângerea depusă de o persoană vizată împotriva unui operator de date. În plus, astfel de plângeri pot fi împărțite în: cazuri naționale fără caracter transfrontalier, cazuri în care se aplică mecanismul ghișeiului unic, deoarece cazul este de natură transfrontalieră și cazuri transfrontaliere care sunt tratate la nivel local în temeiul art. 56 alin. (2) din Regulamentul (UE) 2016/679. Chiar dacă practica arată că soluționările pe cale amiabilă reprezintă un posibil mod de acțiune pentru toate situațiile, Orientările abordează în principal plângerile care au un caracter transfrontalier.

De asemenea, Comitetul european pentru protecția datelor a adoptat o serie de avize comune, împreună cu Autoritatea Europeană pentru Protecția Datelor, după cum urmează:

➤ Avizul comun EDPB-EDPS 1/2022 cu privire la extinderea Regulamentului privind Certificatul Covid-19 extinderea aplicării – prin avizul adoptat, CEPD și AEPD au analizat impactul propunerilor legislative europene care vizează extinderea aplicării Regulamentului (UE) 2021/953 (Certificatul Digital COVID) și, pe cale de consecință, prelungirea Regulamentului (UE) 2021/954 cu 12 luni, precum și prelungirea pentru același interval a competenței Comisiei de a adopta acte delegate în conformitate cu Regulamentul (UE) 2021/953. Propunerile sunt de o importanță deosebită datorită impactului lor major asupra protecției drepturilor și libertăților persoanelor, în ceea ce privește prelucrarea datelor lor personale. Din perspectiva domeniului de aplicare, avizul se limitează la aspectele propunerilor referitoare la protecția datelor cu caracter personal, care reprezintă un aspect fundamental al acestora. Astfel, CEPD și AEPD au reamintit faptul că respectarea prevederilor privind protecția datelor cu caracter personal nu reprezintă un obstacol în lupta contra pandemiei Covid-19 și că, în același timp, principiile generale privind eficacitatea, necesitatea și proporționalitatea trebuie să ghideze orice măsură adoptată de Statele Membre sau instituțiile UE în aspectele ce privesc prelucrarea datelor cu caracter personal în vederea luptei contra Covid-19. Cât privește aspectele specifice, avizul a abordat problema lipsei unui temei pentru analizarea necesității și proporționalității propunerii de regulamente, precum și modificările aduse prelucrărilor curente de date cu caracter personal.

➤ Avizul comun EDPB-EDPS 2/2022 cu privire la Propunerea de Regulament privind normele armonizate în legătură cu accesul echitabil la date și utilizarea lor (Data Act) – prin avizul adoptat, CEPD și AEPD au salutat eforturile făcute pentru a se asigura faptul că Propunerea nu afectează cadrul legislativ actual privind prelucrarea datelor cu caracter personal, considerând, în același timp, că sunt necesare măsuri de protecție suplimentare pentru a se evita scăderea în practică a nivelului de protecție a drepturilor fundamentale la viață privată și la protecția datelor cu caracter personal. Astfel, avizul a abordat chestiuni privind: drepturile la acces, utilizarea și partajarea datelor, obligația de a asigura disponibilitatea datelor în caz de „necesitate excepțională” și implementarea și punerea în executare a prevederilor respective. Întrucât propunerea de regulament, după cum se explică în mod detaliat în aviz, ridică mai multe preocupări cu privire la protecția drepturilor fundamentale la confidențialitate și protecția datelor cu caracter personal, scopul acestuia nu este de a oferi o listă exhaustivă a tuturor problemelor și nici de a oferi întotdeauna propuneri alternative de sugestii de redactare. În schimb, avizul urmărește să abordeze principalele aspecte critice, cu privire la confidențialitatea și protecția datelor din propunere de regulament.

➤ Avizul comun EDPB-EDPS 3/2022 cu privire la Propunerea de Regulament privind Spațiul european de date privind sănătatea – prin avizul adoptat, CEPD și AEPD au reținut că propunerea de regulament urmărește să sprijine persoanele în a prelua controlul asupra propriilor lor date privind starea de sănătate. Totodată, propunerea de regulament susține utilizarea datelor de sănătate pentru o mai bună furnizare a asistenței medicale, o mai bună cercetare, inovare și elaborare a politicilor. Propunerea de regulament prevede în principal câteva „adăugiri” la unele dintre drepturile persoanelor vizate prevăzute de Regulamentul (UE) 2016/679. Or, în fapt propunerea de regulament ar putea chiar să slăbească protecția drepturilor la confidențialitate și protecția datelor, în special având în vedere categoriile de date personale și scopurile care sunt legate de utilizarea secundară a datelor. Întrucât propunerea de regulament, după cum se explică în mod detaliat în aviz, ridică mai multe preocupări cu privire la protecția drepturilor fundamentale la confidențialitate și protecția datelor cu caracter personal, scopul acestuia nu este de a oferi o listă exhaustivă a tuturor problemelor și nici de a oferi întotdeauna propuneri alternative de sugestii de redactare. În schimb, avizul urmărește să abordeze principalele aspecte critice, cu privire la

confidențialitatea și protecția datelor din propunere. De asemenea, avizul analizează interacțiunea propunerii de regulament cu cadrul legislativ general al UE privind protecția datelor cu caracter personal, dar și cu anumite acte normative specifice ale UE – precum Legea privind guvernarea datelor, Legea privind datele și Legea privind Inteligența Artificială.

➤ Avizul comun EDPB-EDPS 4/2022 cu privire la Propunerea de Regulament de stabilire a normelor de prevenire și combatere a abuzului sexual împotriva copiilor

La 11 mai 2022, Comisia Europeană a publicat Propunerea de regulament al Parlamentului European și al Consiliului de stabilire a normelor de prevenire și combatere a abuzului sexual asupra copiilor. Propunerea ar impune obligații specifice furnizorilor de servicii de găzduire, de servicii de comunicații interpersonale și de alte servicii în ceea ce privește detectarea, raportarea, eliminarea și blocarea materialelor online cunoscute și noi care conțin abuzuri sexuale asupra copiilor, precum și ademenirea copiilor și prevede, de asemenea, înființarea unei noi agenții descentralizate a UE („Centrul UE”) și a unei rețele de Autorități naționale de Coordonare pentru problemele legate de abuzul sexual asupra copiilor, pentru a permite punerea în aplicare a propunerii de regulament.

Prin avizul adoptat, CEPD și AEPD au subliniat faptul că propunerea ridică serioase îngrijorări în ceea ce privește proporționalitatea interfețențelor și a limitărilor avute în vedere în raport, cu protecția drepturilor fundamentale la viață privată și cu protecția datelor cu caracter personal. De asemenea, CEPD și AEPD consideră că propunerea de regulament nu este clară în privința unor elemente-cheie, cum ar fi noțiunea de „risc semnificativ”. În plus, entitățile însărcinate cu aplicarea acestor garanții, începând cu operatorii privați și terminând cu autoritățile administrative și/sau judiciare, se bucură de o marjă de apreciere foarte largă, ceea ce duce la insecuritate juridică privind modul de stabilire a echilibrului între drepturile în discuție în fiecare caz în parte. În ceea ce privește necesitatea și proporționalitatea măsurilor de detectare avute în vedere, CEPD și AEPD sunt deosebit de preocupate de măsurile avute în vedere pentru detectarea materialelor necunoscute care conțin abuzuri sexuale asupra copiilor („MASC”) și a cazurilor de ademenire a copiilor („grooming”) în cadrul serviciilor de comunicații interpersonale și își exprimă îndoielile cu privire la eficiența măsurilor de blocare și consideră că solicitarea adresată furnizorilor de servicii de internet de a decripta comunicațiile online pentru a le bloca pe cele referitoare la MASC ar fi disproporționată.



Reguli Corporatiste Obligatorii

Un aspect important în ceea ce privește transferurile internaționale de date cu caracter personal este reprezentat de evaluarea și aprobarea cererilor de reguli corporatiste obligatorii transmise de companii multinaționale. De asemenea, Autoritatea națională de supraveghere are un rol consultativ în privința transferurilor de date, indiferent de temeiul legal al acestora.

Reguliile corporative obligatorii (BCRs) au fost introduse ca răspuns la nevoia organizațiilor de a avea o abordare globală în ceea ce privește protecția datelor cu caracter personal, în situația în care multe organizații dețineau mai multe filiale/sucursale situate pe tot globul, transferând date cu caracter personal la scară largă. Incluzând BCRs în Regulamentul (UE) 2016/679 consolidează în continuare utilizarea lor ca garanție adecvată pentru a legitima transferurile de date cu caracter personal în țări terțe.

În anul 2022, Autoritatea națională de supraveghere a primit și a analizat cereri de aprobare a BCRs, transmise de 34 companii multinaționale. De asemenea, Autoritatea națională de supraveghere a asistat alte autorități de supraveghere, acționând în calitate de co-revizor la cererile de aprobare a BCRs, transmise de 4 companii în această perioadă și ca membru în echipa de redactare a 3 propuneri de opinie a Comitetului European pentru Protecția Datelor referitoare la adoptarea regulilor corporatiste obligatorii.

În calitate de autoritate principală și autoritate co-revizor, Autoritatea națională de supraveghere a formulat o serie de observații și recomandări dintre care evidențiem următoarele:

- includerea definițiilor pentru cei mai uzitați termeni din domeniul protecției datelor cu caracter personal,
- menționarea în mod expres a categoriilor de date cu caracter personal prelucrate și transferate în temeiul clauzei corporatiste obligatorii,
- stabilirea unei proceduri pentru situația în care cererile persoanelor vizate sunt primite de alte departamente/persoane, precum și a termenilor de redirecționare a respectivelor cereri,
- păstrarea unei evidențe a cererilor de exercitare a drepturilor de la persoanele vizate,
- păstrarea unei evidențe a plângerilor primite de la persoanele vizate și întocmirea de către responsabilul cu protecția datelor a unui raport referitor la plângerile primite, obiectul plângerilor, precum și rezultatul soluționării acestora,



➢ includerea de mențiuni referitoare la dreptul de a se opune în contextul prelucrării datelor cu caracter personal în scop de marketing direct, informarea persoanei vizate, în mod explicit, în legătură cu acest drept, posibilitatea de exercitare a dreptului de a se opune prin mijloace automate care utilizează specificații tehnice, în contextul utilizării serviciilor societății informaționale,

➢ includerea de mențiuni exprese cu privire la dreptul persoanei vizate de a depune o plângere la Autoritatea națională de supraveghere în situația în care nu primește un răspuns/nu este mulțumit de răspunsul primit de la operator,

➢ păstrarea unei evidențe actualizată a modificărilor aduse regulilor corporatiste obligatorii,

➢ menționarea principiilor legate de prelucrarea datelor cu caracter personal, utilizând formularea din Regulamentul (UE) 2016/679,

➢ includerea de mențiuni referitoare la excepțiile de la furnizarea de informații către persoana vizată atunci când datele nu au fost obținute de la aceasta,

➢ includerea tuturor scenariilor în care se aplică dreptul de ștergere prevăzut de art. 17 din Regulamentul (UE) 2016/679,

➢ specificarea în mod clar a modalității de păstrare a evidenței activităților de prelucrare, ce informații vor fi incluse în respectiva evidență etc., în conformitate cu art. 30 din Regulamentul (UE) 2016/679.

Procedura de aprobare a BCRs s-a modificat de la un sistem de recunoaștere reciprocă în conformitate cu Directiva 95/46/CE, la sistemul actual în care toate BCRs trebuie să fie prezentate Comitetului european pentru protecția datelor, în vederea obținerii unui aviz în temeiul art. 64 din Regulamentul (UE) 2016/679.

Această procedură presupune că toate autoritățile de supraveghere au posibilitatea de a transmite observații pe marginea cererilor BCRs, ceea ce duce la o procedură de cooperare ceva mai lungă. Procedura va ajuta Comitetul european pentru protecția datelor la redactarea avizului său dacă toate chestiunile problematice sunt soluționate înainte de demararea procedurii prevăzute la art. 64 din Regulamentul (UE) 2016/679. În anul 2022, Comitetul european pentru protecția datelor a emis 23 de avize în temeiul art. 64 din Regulamentul (UE) 2016/679, pe marginea proiectelor de decizie înaintate de autoritățile de supraveghere referitoare la regulile corporatiste obligatorii.



Solicitați de asistență reciprocă prin intermediul sistemului IMI

În contextul cooperării cu alte autorități de supraveghere din UE în vederea asigurării asistenței reciproce, au fost gestionate solicitări cu privire la aplicarea și respectarea Regulamentului (UE) 2016/679. Solicitățile venite din partea autorităților de supraveghere din Austria, Franța, Germania, Irlanda, Letonia, Malta, Norvegia, Polonia, Slovacia, Slovenia au vizat aspecte referitoare la prelucrarea datelor prin intermediul sistemelor cu circuit închis, prelucrarea datelor biometrice în penitenciare, interdicția de concediere a responsabilității cu protecția datelor, monitorizarea și localizarea numerelor de înmatriculare, criteriile pentru prioritizarea plângerilor, transpunerea prevederilor art. 25 din Directiva (UE) 2016/680, independența autorităților de supraveghere.

Contribuții din perspectiva protecției datelor cu caracter personal

În cursul anului 2022, Autoritatea națională de supraveghere a formulat observații și propuneri pe marginea documentelor transmise de alte autorități/instituții:

➤ raportul anual 2021 și planul de lucru 2023 al Agenției pentru Drepturi Fundamentale a Uniunii Europene – Autoritatea națională de supraveghere a transmis comentarii pe marginea celor două documente transmise spre analiză, cu incidență asupra capitolului care vizează domeniul protecției datelor cu caracter personal;

➤ propunerea de regulament privind înființarea unui cadru pentru identitatea digitală europeană (EIDAS) – În ceea ce privește furnizarea de identitate digitală, inclusiv emiterrea unui portofel european de identitate digitală și infrastructura pentru colectarea, stocarea și dezvăluirea datelor de identitate digitală, autoritatea națională de supraveghere a subliniat faptul că este necesar să se asigure un nivel ridicat de securitate tuturor aspectelor ce țin de identitatea digitală. De asemenea, având în vedere complexitatea și sensibilitatea datelor cu caracter personal cuprinse în portofelele europene de identitate digitală, precum și asigurarea la care acestea se vor emite și utiliza, Autoritatea națională de supraveghere a considerat oportună includerea nominală a unui set minim de standarde privind securizarea cibernetică, cu adresabilitate directă prestatorilor de servicii de încredere calificată. În plus, referitor la propunerea de modificare a art. 17 alin. (4) litera f), Autoritatea națională de supraveghere a atras atenția asupra faptului că, în temeiul art. 33 din Regulamentul (UE) 2016/679, operatorul are obligația de a notifica autoritatea pentru protecția datelor cu privire la



incălcările de securitate și nu Organismul de Supraveghere desemnat în temeiul Regulamentului (UE) nr. 910/2014. Astfel, autoritatea pentru protecția datelor va fi informată de Organismul de Supraveghere atunci când acesta primește informații despre o posibilă încălcare a securității datelor. Din aceleași considerente ca cele menționate anterior, art. 20 alin. (2) ar trebui, de asemenea, aliniat la prevederile Regulamentului (UE) 2016/679. În plus, s-a considerat că autoritățile pentru protecția datelor ar trebuie informate cu privire la încălcările securității datelor, indiferent dacă auditul a fost finalizat sau se află în curs de desfășurare. Totodată, în contextul creării unui identificator unic și constant care ar putea intra sub sfera definiției conceptului de „date cu caracter personal”, astfel cum este definit la art. 4 punctul 1 din Regulamentul (UE) 2016/679, Autoritatea națională de supraveghere a apreciat că devin aplicabile prevederile art. 87 din Regulamentul (UE) 2016/679, respectiv obligativitatea folosirii acestuia numai în temeiul unor garanții corespunzătoare pentru drepturile și libertățile persoanei vizate, cu mențiunea că art. 87 din Regulamentul (UE) 2016/679 a fost implementat la nivel național prin art. 4 din Legea nr. 190/2018. De asemenea, în situația în care se va utiliza identificatorul unic și constant pentru EIDW, Autoritatea națională de supraveghere a subliniat faptul că un astfel de identificator oferă posibilitatea accesării informațiilor conexe și reționate în momentul folosirii acestuia pentru utilizarea de servicii de orice fel. Acest fapt impune o securizare sporită a procesului de identificare electronică și a atributelor adiacente, având în vedere categoriile de date cu caracter personal ce ar putea fi accesate în mod neautorizat, precum și conformitatea în ceea ce privește toate exigențele prevăzute de Regulamentul (UE) 2016/679. Pentru situațiile privind identificarea electronică via EDIW *in situ*, din punct de vedere tehnic, se impune securizarea de tip „multifactor authentication” și nu ar putea fi posibilă dacă EDIW se va rezuma doar la integrarea într-un dispozitiv smartphone, în contextul în care acel al doilea factor de verificare reprezintă de cele mai multe ori un cod de securizare primit via email/sms. Pentru reducerea riscului furtului de identitate, identificarea electronică, împreună cu alte atribute adiacente, trebuie să se bazeze pe autorizarea generată de cel puțin două dispozitive tip hardware (fie un cont securizat plus cod securizare transmis pe smartphone pentru servicii online sau, spre exemplu, pentru identificarea *in situ* un smartphone plus cod securizare generat de un dispozitiv token);

➤ propunerea de regulament de stabilire a unor norme armonizate privind inteligența artificială – Autoritatea națională de supraveghere a considerat că propunerea de regulament



privind inteligența artificială are implicații importante asupra protecției datelor cu caracter personal, subliniind faptul că dreptul la viață privată și dreptul la protecția datelor cu caracter personal reprezintă un pilon al valorilor UE, așa cum sunt recunoscute în Declarația Universală a Drepturilor Omului (art. 12), Convenția Europeană a Drepturilor Omului (art. 8) și Carta Drepturilor Fundamentale a UE (art. 7 și 8). Deși considerentele propunerii de regulament clarifică faptul că utilizarea sistemelor de inteligență artificială ar trebui să respecte în continuare legislația privind protecția datelor, Autoritatea națională de supraveghere a recomandat clarificarea în cuprinsul propunerii de regulament că legislația privind protecția datelor cu caracter personal, în special Regulamentul (UE) 2016/679, se aplică oricărei prelucrări de date cu caracter personal care se încadrează în domeniul de aplicare al propunerii de regulament. De asemenea, Autoritatea națională de supraveghere a considerat ca fiind necesară menționarea în mod expres, în cuprinsul propunerii de regulament, a drepturilor și a căilor de atac disponibile persoanelor vizate care fac obiectul sistemelor de inteligență artificială, astfel cum sunt prevăzute în Regulamentul (UE) 2016/679. Referitor la Titlul III – Sisteme de IA cu grad ridicat de risc, s-a recomandat includerea în Capitolul II a cerinței de a asigura conformitatea cu Regulamentul (UE) 2016/679. Utilizarea datelor cu caracter personal pentru sisteme de inteligență artificială poate duce la generarea de diferite modele de luare a deciziilor. Astfel, Autoritatea națională de supraveghere a considerat că ar trebui să existe garanții concrete, detaliate, fiind necesară totodată și o supraveghere umană calificată în astfel de procese pentru a se asigura că drepturile persoanelor vizate sunt respectate și garantate, precum și pentru a evita orice efect negative pentru persoanele fizice. În acest sens, s-a atras atenția inclusiv asupra modului de formulare al alin. (5) al art. 10 „(...) sub rezerva unor garanții adecvate pentru drepturile și libertățile persoanelor fizice (...)”. Persoanele vizate ar trebui să fie întotdeauna informate clar atunci când datele lor sunt utilizate pentru sistemele de inteligență artificială, să fie informate în legătură cu temeiul legal pentru o astfel de prelucrare, în legătură cu explicație generală a logicii folosite (procedura) și domeniul de aplicare al sistemului de inteligență artificială, fără a se folosi sintagme vagi precum „să fie informate (...) cu excepția cazului în care acest lucru este evident din circumstanțele și contextul de utilizare (...)” (a se vedea spre exemplu art. 52 alin. (1)). În această privință, dreptul persoanelor la restricționarea prelucrării (art. 18 din Regulamentul (UE) 2016/679), precum și dreptul la ștergerea datelor (art. 17 din Regulamentul (UE) 2016/679) ar trebui să fie întotdeauna



garantate în aceste cazuri. În plus, operatorul ar trebui să aibă obligația explicită de a informa persoana vizată cu privire la exercitarea dreptului la restricționare, a dreptului la ștergerea datelor etc. Sistemele de inteligență artificială trebuie să fie capabile să respecte toate cerințele privind protecția datelor cu caracter personal prin măsuri tehnice și organizatorice adecvate. Astfel, Autoritatea națională de supraveghere a subliniat necesitatea includerii de mențiuni referitoare la drepturile de care beneficiază persoanele vizate în temeiul Regulamentului (UE) 2016/679 (dreptul la informare, dreptul la restricționare, dreptul la ștergere etc.), precum și la modalitatea și condițiile de exercitare a acestora. Referitor la art. 54 alin. (1), a fost evidențiată importanța respectării tuturor principiilor de prelucrare a datelor cu caracter personal, cu precădere a celui prevăzut la art. 5 alin. (1) litera b) potrivit căruia datele nu pot fi prelucrate ulterior într-un mod incompatibil cu scopul legal declarat inițial („limitări legate de scop”), sens în care s-a considerat necesară reformularea prevederilor de la art. 54 alin. (2) din propunerea de regulament. De asemenea, Autoritatea națională de supraveghere a apreciat că se impune includerea de prevederi explicite referitoare la obligația de a implementa măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, precum și împotriva oricărei alte forme de prelucrare ilegală. Spre exemplu, Autoritatea națională de supraveghere a considerat oportună completarea alin. (4) al art. 12 cu elementele obligatorii care trebuie asigurate de capacitățile de jurnalizare ale unui sistem de inteligență artificială de risc ridicat, în sensul instituirii trasabilității anumitor acțiuni care privesc copierea sau transferul de date cu caracter personal în afara acestuia, inclusiv prin emiterea de alerte. În plus, având în vedere sensibilitatea problematicii, respectiv inteligența artificială, Autoritatea națională de supraveghere a atras atenția asupra necesității asigurării protecției datelor începând cu momentul concepției și în mod implicit, principiile privacy by design și privacy by default statuate de art. 25 din Regulamentul (UE) 2016/679. Cu privire la dispozițiile din propunerea de regulament, a fost evidențiat faptul că operatorii de date, potrivit principiului „responsabilității” stipulat la art. 5 alin. (2) din Regulamentul (UE) 2016/679, nu numai că sunt responsabili de respectarea tuturor principiilor de prelucrare a datelor cu caracter personal, dar este necesar ca aceștia să poată demonstra, efectiv, respectarea acestora. Prin urmare, în opinia autorității de supraveghere, este important să se evite în mod clar orice inconsecvență cu Regulamentul (UE) 2016/679;



➤ propunere de regulament de stabilire a normelor de prevenire și combatere a abuzului sexual împotriva copiilor – Autoritatea națională de supraveghere a evidențiat faptul că orice limitări ale drepturilor fundamentale, precum cele prevăzute în propunerea de regulament, trebuie să respecte cerințele prevăzute la articolul 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene. Astfel, Autoritatea națională de supraveghere a subliniat faptul că respectiva propunere are implicații deosebite din punct de vedere al principiului proporționalității, precum și a limitărilor aduse dreptului la protecția datelor cu caracter personal și a dreptului la viață privată. Prin urmare, pentru a fi putea evalua impactul unei măsuri asupra drepturilor fundamentale la viața privată și la protecția datelor cu caracter personal, este deosebit de important să se identifice domeniul de aplicare al măsurii, inclusiv numărul de persoane afectate (persoane vizate), volumul de date cu caracter personal și perioada de stocare a acestora, inclusiv mențiuni privind prelucrarea sau nu a unor categorii speciale de date cu caracter personal, nivelul de intruziune, dacă vizează persoane vulnerabile sau nu (minorii intrând în această categorie), dacă sunt afectate și alte drepturi fundamentale. Referitor la principiul necesității și proporționalității măsurilor de detectare prevăzute în propunerea de regulament, Autoritatea națională de supraveghere și-a manifestat îngrijorarea în ceea ce privește măsurile avute în vedere pentru detectarea materialelor de abuz sexual asupra copiilor necunoscute, având în vedere caracterul intruziv al acestora din cauza posibilității acordării accesului la conținutul comunicațiile pe o bază generalizată. În același timp, propunerea de regulament stabilește anumite tehnologii care urmează să fie implementate pentru detectarea de materiale de abuz sexual asupra copiilor. Astfel, s-a considerat necesară includerea în mod expres a principiului privacy by design și privacy by default care să se aplice tehnologiilor stabilite prin propunerea de regulament. Când privește principiul limitării legate de stocare, s-a recomandat stabilirea de termene maxime de păstrare a datelor cu caracter personal sau, cel puțin, a unui termen maxim pentru revizuirea necesității păstrării în continuare a datelor cu caracter personal. În ceea ce privește drepturile persoanelor vizate, Autoritatea națională de supraveghere nu a identificat în propunerea de regulament prevederi pentru exercitarea drepturilor persoanelor vizate, având în vedere și varietatea de destinații ai datelor cu caracter personal colectate. Așadar, cerința de a informa utilizatorii ar trebui să includă obligația de a informa persoanele vizate că datele lor au fost transmise și sunt prelucrate de diferite entități, acolo unde este cazul. În plus, ar



trebui să existe o procedură clar stabilită pentru primirea și soluționarea cererilor persoanelor vizate prin care acestea își exercită dreptul de acces, rectificare și ștergere;

➤ chestionar tematic al Raportorului special privind dreptul la respectarea vieții private în coordonarea Consiliului Drepturilor Omului al Organizației Națiunilor Unite – Autoritatea națională de supraveghere a transmis contribuția sa în vederea pregătirii raportului tematic dedicat protecției datelor cu caracter personal și folosirii, păstrării și ștergerii acestor tipuri de date colectate de către guvernele statelor membre în timpul pandemiei de COVID-19;

➤ chestionar privind stadiul implementării art. 65 din Directiva (UE) 2018/843 – Autoritatea națională de supraveghere a transmis informații referitoare la activitatea de consultare legislativă pe marginea propunerilor de acte normative de transpunere sau implementare a directivei privind spălarea banilor, precum și informații privind plângerile primite care au avut ca obiect adiacent cerințele Directivei (UE) 2018/843;

➤ reuniune cu reprezentanți ai Biroului pentru Instituții Democratice și Drepturile Omului (ODIHR) – reuniunea a avut loc în contextul celui de-al doilea ciclu de evaluare la nivel de țară privind situația apărătorilor drepturilor omului. Procesul de evaluare privind situația apărătorilor drepturilor omului a fost lansat de către ODIHR pentru a analiza implementarea în statele vizitate a Ghidului ODIHR pentru protecția apărătorilor drepturilor omului, document care codifică standardele internaționale și angajamentele ODIHR în materie. Aceste linii directoare se bazează pe angajamentul de lungă durată al Biroului OSCE pentru Instituții Democratice și Drepturile Omului (ODIHR) față de apărătorii drepturilor omului și au ca scop sprijinirea statelor participante în punerea în aplicare a angajamentelor privind dimensiunea umană legate de protecția apărătorilor drepturilor omului;

➤ interviu și reuniuni cu reprezentanți ai Observatorului Spațiului Civic al Organizației pentru Cooperare și Dezvoltare Economică (OCDE) – Autoritatea națională de supraveghere a participat la reuniunile organizate de OCDE, cu sprijinul Secretariatului General al Guvernului, care au avut loc în vederea scanării spațiului civic al României și pentru dezvoltarea unei strategii și a unei foi de parcurs pentru implementare, cu scopul implicării societății civile în procesul decizional. Pentru atingerea obiectivelor propuse, au fost derulate o serie de activități de colectare de informații de autorități și instituțiile publice și societatea civilă, care au fost incluse în raportul OCDE privind spațiul civic al României;

> procesul de autoevaluare a implementării instrumentelor juridice ale OCDE – în cadrul procesului de aderare a României la Organizația pentru Cooperare și Dezvoltare Economică (OCDE), ca urmare a inițierii procesului de autoevaluare a implementării instrumentelor juridice ale OCDE, Autoritatea națională de supraveghere a transmis o serie de propuneri și observații pe marginea fișelor de autoevaluare cu incidență în domeniul protecției datelor cu caracter personal, acestea cuprinzând informații privind legislația (informații care argumentează felul în care legislația este aliniată cu instrumentul), politici (informații privind felul în care politicile guvernamentale corespund instrumentului), practici (informații privind felul în care practicile corespund instrumentului);

> vizită de evaluare Schengen în domeniul protecției datelor – rezultatele activității desfășurate de Autoritatea națională de supraveghere se reflectă, în mod favorabil, în raportul misiunii voluntare de constatare privind aplicarea acquis-ului Schengen în România, vizită de evaluare Schengen realizată de experți ai statelor membre, sub coordonarea Comisiei Europene. Astfel, cu ocazia vizitei derulate în luna noiembrie 2022, experții evaluatori au menționat faptul că au fost înregistrate progrese importante pentru aplicarea integrală a acquis-ului Schengen în România.

CAPITOLUL V

MANAGEMENTUL ECONOMIC AL AUTORITĂȚII

În vederea desfășurării activității, Autorității naționale de supraveghere i s-a alocat prin Legea nr. 317/2021 a bugetului de stat pe anul 2022 un buget inițial în sumă de 5.336.000 lei, modificat în conformitate cu prevederile Ordonanței Guvernului nr. 19/2022 cu privire la rectificarea bugetului de stat pe anul 2022 și Ordonanței de Urgență a Guvernului nr. 160/2022 cu privire la rectificarea bugetului de stat pe anul 2022.

Evoluția sumelor alocate pentru bugetul Autorității naționale de supraveghere în ultimii 5 ani poate fi observată în tabelul de mai jos:

Comparație buget anual 2018-2022

| Anul | 2018 | 2019 | 2020 | 2021 | 2022 |
|-------------------------|----------|---------|--------|--------|---------|
| Buget final (mii lei) | 4.735 | 5.147 | 4.903 | 4.601 | 5580 |
| % fata de anul anterior | 110,45 % | 108,70% | 95,26% | 93,84% | 121,27% |

Bugetul anului 2022 a fost mai mare cu aproximativ 21% față de bugetul anului anterior. Dat fiind faptul că modul de concepere a bugetelor pune un accent semnificativ pe sumele cheltuite anterior, din cauza numărului mic de personal și a faptului că sumele necesare depășesc semnificativ alocările anterioare la capitolul investiții, bugetele aprobate pentru Autoritatea națională de supraveghere au rămas la un nivel care asigură, în principal, funcționarea și doar în mică măsură dezvoltarea.

Anul 2022 a fost o excepție de la trendul descrescător al sumelor alocate Autorității, datorită eliminării în prima parte a anului, a restricțiilor generate de pandemia COVID-19 și, mai ales, creșterii cheltuielilor din cauza evoluției ascendente a prețurilor, în urma conflictului armat din Ucraina. Creșterea prețurilor, atât la utilități cât și la alte bunuri s-a reflectat în necesități mai mari de fonduri pe toate titlurile de cheltuieli din bugetul Autorității naționale de supraveghere.



În anul 2022, un impact semnificativ asupra cheltuielilor l-au avut, așa cum se menționează mai sus, costurile crescute, atât cele ale utilităților cât și cele ale bunurilor și serviciilor necesare pentru funcționarea Autorității naționale de supraveghere, precum și cele cu realizare unor investiții minim necesare în infrastructura IT.

Având în vedere aceste aspecte, în urma modificărilor de alocări bugetare realizate prin actele normative de rectificare a bugetului de stat pe anul 2022 și în urma anulațiilor de credite realizate în luna decembrie 2022, conform reglementărilor Legii nr. 500/2002 privind finanțele publice, rezultă următoarea sinteză:

| Denumire indicator | Cod | Buget inițial 2022 - mil lei - | Buget final (actualizat la 31.12.2022) - mil lei - | Execuție bugetară la 31.12.2021 - mil lei - | Execuție bugetară la 31.12.2021 (%) |
|---------------------------------|-------|--------------------------------------|--------------------------------------------------------------------|------------------------------------------------------|----------------------------------------------|
| Total cheltuieli | 51.01 | 5.336 | 5.580 | 5.537,5 | 99,23 |
| Titlul I Cheltuieli de personal | 10 | 4.300 | 4.599 | 4.586,8 | 99,73 |
| Titlul II Bunuri și servicii | 20 | 904 | 861 | 835,3 | 97,01 |
| Cheltuieli de capital | | | | | |
| Titlul XIII Active nefinanciare | 71 | 132 | 120 | 116,4 | 97,00 |

Întrucât pe parcursul exercițiului bugetar au avut loc rectificări bugetare, s-a urmărit permanent actualizarea priorităților pentru realizarea celor mai importante proiecte cu fondurile disponibile.

În prima parte a anului 2022 pandemia COVID-19 a avut încă un impact asupra activităților instituției, în această perioadă fiind diminuate deplasările personalului și existând în continuare preocuparea pentru limitarea expunerii la îmbolnăvire a salariaților.



În partea a doua a anului 2022 cheltuielile au fost influențate, în mare măsură, de impactul creșterii prețurilor la utilități, bunuri și servicii necesare desfășurării activității. În acest context, s-au luat măsuri organizatorice și s-a încercat, în măsura posibilităților, utilizarea cu maximă eficiență a fondurilor bugetare aprobate și realizarea achizițiilor amânate din perioada de vârf a pandemiei (nerealizate sau întârziate din cauza problemelor aferente aprovizionării cu materii prime, de logistică și transport).

În acest context, creditele definitive alocate instituției au asigurat continuitatea activității Autorității de supraveghere, fiind dispuse de conducerea instituției măsuri interne privind utilizarea eficientă a fondurilor publice.

În ceea ce privește modul de repartizare a fondurilor alocate, precizăm că suma aferentă cheltuielilor de personal ale Autorității naționale de supraveghere a constituit un procent de 82,41% din totalul creditelor repartizate de la bugetul de stat, din care s-au utilizat efectiv credite în valoare de 4.586,8 mil lei.

Autoritatea națională de supraveghere a continuat să înregistreze și în anul 2022 un deficit major de personal, numărul mediu al posturilor ocupate fiind de 36 din totalul de 87 prevăzut de Legea nr. 102/2005 republicată (doar 33 posturi ocupate la debutul anului și 35 posturi ocupate la finalul anului 2022 – inclusiv demnitarii).

Majoritatea cheltuielilor de personal au fost aferente plăților efectuate pentru munca salariată a angajaților din compartimentele de specialitate.

Cheltuielile aferente titlului Bunuri și servicii în anul 2022 au avut o pondere de 15,43% în bugetul instituției, iar din acestea, cheltuielile cu pondere mai importantă au fost:

- I. aproximativ 49,26% din totalul sumelor achitate din conturile de trezorerie ale Autorității la titlul II Bunuri și servicii au fost reprezentate de costurile de închiriere și cheltuielile cu utilitățile și serviciile prestate de RA-APPS prin intermediul SAIFI,
- II. diferența până la 100% este reprezentată de cheltuieli cu bunuri și servicii pentru întreținere și funcționare (servicii de actualizare informatică, servicii de suport tehnic, instalare și configurare software, actualizarea sistemului electronic de gestiune a documentelor FoliuM, curățenie, cheltuieli cu serviciile poștale și de telefonie, cheltuieli generate de pandemie, abonament program legislativ, furnituri de birou și alte materiale necesare desfășurării activității etc.).



În anul 2022, cheltuielile cu bunuri și servicii au crescut cu 18,04 % față de anul 2021, în contextul majorărilor semnificative a prețurilor (execuția bugetară la titlul II Bunuri și servicii fiind de 835,3 mii lei în anul 2022, față de 707,6 mii lei în anul 2021).

Pe parcursul exercițiului bugetar 2022, datorită unor circumstanțe neprevăzute, necesarul de fonduri s-a modificat, iar lista de investiții a suferit schimbări față de estimările inițiale, ceea ce a determinat o execuție bugetară ușor diferită față de previziunile realizate cu prilejul întocmirii proiectului de buget pe anul 2022.

De asemenea, trebuie precizat că, în măsura în care acest lucru a fost posibil, s-au avut permanent în vedere factori precum: oportunitatea cheltuielilor, criteriul prețului celui mai scăzut aplicat în procedurile de achiziții publice, alăturat unor cerințe tehnice atent stabilite – ceea ce a condus la utilizarea eficientă a fondurilor bugetare alocate atât la Titlul II Bunuri și servicii cât și la Titlul XIII Active nefinanciare.

În ceea ce privește Titlul XIII Active nefinanciare, în anul 2022 Autoritatea națională de supraveghere a continuat – în măsura posibilităților oferite de alocările bugetare și de situațiile generate de unele probleme ale sistemului IT – proiectul de reînnoire a infrastructurii, în aceste scopuri fiind utilizate fondurile prevăzute în bugetul final al titlului Cheltuieli de capital. Acest proiect continuă să fie deosebit de important, funcționarea sistemului IT fiind esențială în contextul trecerii într-o proporție tot mai mare a activității în mediul on-line, datorită pandemiei și a tendințelor de la nivel intern și internațional.

Politicile contabile utilizate la întocmirea situațiilor financiare anuale sunt în conformitate cu reglementările legale în vigoare, iar situațiile financiare anuale oferă o imagine fidelă a realității poziției financiare a Autorității naționale de supraveghere, precum și informații privind încadrarea în creditele bugetare alocate pe grupe, titluri, articole și alineate de cheltuieli. Cheltuielile bugetare s-au efectuat cu respectarea principiilor privind legalitatea, oportunitatea, continuitatea și eficiența. Toate documentele care intră sub incidența controlului financiar preventiv propriu au fost verificate și vizate pentru conformitate/încadrare în limitele bugetare.

Ca o concluzie asupra gestionării fondurilor bugetare alocate, putem preciza că acestea au fost utilizate cu maximum de eficiență posibil într-o perioadă ce a continuat să fie plină de provocări și că sumele cuprinse în bugetul instituției au făcut obiectul unei atențe administrări.



CAPITOLUL VI

PROPUNERI DE LEGE FERENDA

- **Propunere de completare a Constituției României în perspectiva unei reforme constituționale**

În considerarea reglementărilor europene, propunem adăugarea în categoria drepturilor fundamentale a dreptului la protecția datelor cu caracter personal, ca drept distinct, alături de art. 26 din Constituție privind dreptul la viață intimă, familială și privată, în concordanță cu prevederile art. 16 din Tratatul de Funcționare a Uniunii Europene.

Ca efect al aplicării și impactului Regulamentului (UE) 2016/679, propunem includerea în Constituția României a unui articol privind Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, competențele și rolul acesteia de apărător al dreptului la viață privată și al dreptului la protecția datelor cu caracter personal ale persoanelor fizice, după articolul referitor la instituția Avocatului Poporului.

- **Propunere de modificare a Legii nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)**

Semnalăm necesitatea abrogării art. 6 și art. 9 din Legea nr. 190/2018 întrucât nu sunt în concordanță cu prevederile referitoare la condițiile de legalitate stabilite prin Regulamentul (UE) 2016/679.

Astfel, este necesară abrogarea art. 6 din Legea nr. 190/2018, întrucât acesta produce o confuzie de fond privind temeiurile de prelucrare și folosește o terminologie inadecvată ("date personale și speciale"), prin raportare la definițiile din art. 4 pct. 1, art. 4 pct. 10, art. 9 din Regulamentul (UE) 2016/679.

De asemenea, considerăm că este necesară abrogarea art. 9 din Legea nr. 190/2018, întrucât situația stabilită de acest text nu se regăsește în sfera condițiilor de legalitate vizate de art. 6 și art.9 din Regulamentul (UE) 2016/679, coroborat cu mențiunile din considerentele (45), (47) și (56) ale aceluiași regulament.

Este de observat faptul că Regulamentul (UE) 2016/679 se referă doar la partidele politice, nu și alte entități, cum sunt cele menționate de art. 9 din Legea nr. 190/2018, respectiv organizațiile cetățenilor aparținând minorităților naționale și organizațiile neguvernamentale, iar scopul prelucrării stabilit de reglementarea europeană este numai "din motive de interes public", nu pentru orice obiectiv urmărit, așa cum stabilește art. 9 din Legea nr. 190/2018.

Mai mult, față de cele stabilite de Regulamentul (UE) 2016/679, art. 9 din Legea nr. 190/2018 nu respectă condițiile stabilite de legiuitorul european și nu asigură proporționalitatea și echilibrul despre care se face vorbire în textul acestui articol.

În plus, Regulamentul (UE) 2016/679 obligă la asigurarea unor garanții corespunzătoare ceea ce nici art. 9 și nici art. 6 din Legea nr. 190/2018 nu conține.

În consecință, este necesară abrogarea art. 6 și art. 9 din Legea nr. 190/2018, ținând cont de implicațiile Legii nr. 190/2018 în asigurarea unei aplicări corecte a Regulamentului (UE) 2016/679, act obligatoriu în toate elementele sale.

Pe de altă parte, pentru claritatea normei, propunem modificarea art. 13 alin. 3 din Legea nr. 190/2018, astfel:

„După 10 zile de la data expirării termenului de remediere, Autoritatea națională de supraveghere poate să rela controlului.”

- *Propunere de modificare a art. 14 Legea nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date*

Raportat la asigurarea unei reale respectări a dreptului la informare al persoanelor vizate, semnalăm necesitatea eliminării sintagmei "la cerere", prevăzută la art. 14 din Legea nr. 363/2018, pentru a asigura o corectă transpunere a prevederilor art. 12-13 din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului.

Astfel, subliniem că Directiva (UE) 2016/680 nu condiționează respectarea dreptului de informare de existența unei cereri prealabile, iar importanța recunoașterii drepturilor persoanelor vizate în privința prelucrării datelor personale conduce la necesitatea modificării corespunzătoare a prevederilor art. 14 din Legea nr. 363/2018.

